S-02

SEIKO EPSON

PP-100N Security Control Unit Security Target

Version 2.0

2009-07-03

This document is a translation of the evaluated and certified security target written in Japanese.

SEIKO EPSON CORPORATION

Table of Contents

1 ST SECURITY TARGET (ST) OVERVIEW 5

1.1 ST IDENTIFICATION 5
1.2 ST OVERVIEW 5
1.3 CC CONFORMANCE 6
1.4 TERMINOLOGY AND ACRONYMS 6
1.5 TRADEMARKS 8

2 TOE DESCRIPTION 9

2.1 TOE OVERVIEW 9
2.1.1 TYPE OF PRODUCT 9
2.1.2 INTENDED USE 9
2.1.3 ENVIRONMENT OF USE 9
2.2 PARTIES INVOLVED WITH TOE 10
2.3 PHYSICAL CONFIGURATION 11
2.3.1 HARDWARE CONFIGURATION 11
2.3.2 HARDWARE COMPONENTS 11
2.3.3 HARDWARE OF THE TOE 13
2.3.4 SOFTWARE CONFIGURATION 13
2.3.5 SOFTWARE COMPONENTS 14
2.3.6 TOE RANGE OF THE SOFTWARE 15
2.4 LOGICAL CONFIGURATION 15
2.4.1 LOGICAL CONFIGURATION 15
2.4.2 LOGICAL COMPONENTS 16
2.4.3 LOGICAL SCOPE AND BOUNDARY OF THE TOE 17
2.5 PROTECTED ASSETS 17
2.6 TOE FUNCTIONALITY 18
2.6.1 TOE FUNCTIONS 18
2.6.2 USAGE 20
2.6.3 OPERATIONAL PROCEDURE 22
2.7 EVALUATION CONFIGURATION 24

3 TOE SECURITY ENVIRONMENT 25

3.1 ASSUMPTIONS 25
3.2 THREATS 25

3.3 ORGANIZATIONAL SECURITY POLICIES 26

4 SECURITY OBJECTIVES 27

4.1 SECURITY OBJECTIVES FOR THE TOE 27
4.2 SECURITY OBJECTIVES FOR THE ENVIRONMENT 27

5 IT SECURITY REQUIREMENTS 29

5.1 TOE SECURITY REQUIREMENTS 29
5.1.1 TOE SECURITY FUNCTIONAL REQUIREMENTS 29
5.1.2 TOE SECURITY ASSURANCE REQUIREMENTS 42
5.1.3 MINIMUM STRENGTH OF FUNCTION 43
5.2 IT SECURITY REQUIREMENTS FOR THE IT ENVIRONMENT 43

6 TOE SUMMARY SPECIFICATION 44

6.1 TOE SECURITY FUNCTIONS 44
6.1.1 TOE SECURITY FUNCTIONS 44
6.1.2 TOE SECURITY FUNCTION STRENGTH 50
6.2 ASSURANCE MEASURES 51

7 PP CLAIMS 52

8 RATIONALE 53

8.1 SECURITY OBJECTIVES RATIONALE 53
8.1.1 NEED OF SECURITY OBJECTIVES 53
8.1.2 SUFFICIENCY OF SECURITY OBJECTIVES 53
8.2 SECURITY REQUIREMENTS RATIONALE 55
8.2.1 NEED OF SECURITY FUNCTIONAL REQUIREMENTS 55
8.2.2 SUFFICIENCY OF SECURITY FUNCTIONAL REQUIREMENTS 57
8.2.3 ADEQUACY OF SECURITY FUNCTIONAL REQUIREMENTS DEPENDENCIES 59
8.2.4 INTERRELATIONSHIPS AMONG SECURITY FUNCTIONAL REQUIREMENTS 61
8.2.5 ADEQUACY OF MINIMUM STRENGTH OF FUNCTION 63
8.2.6 ADEQUACY OF EVALUATION ASSURANCE LEVEL 63
8.2.7 RATIONALE FOR SECURITY ASSURANCE REQUIREMENTS 63
8.2.8 RATIONALE FOR SECURITY FUNCTIONAL REQUIREMENTS CONSISTENCY 63
8.3 TOE SUMMARY SPECIFICATION RATIONALE 64

8.3.1 NEEDS OF TOE SECURITY FUNCTIONS 64
8.3.2 SUFFICIENCY OF TOE SECURITY FUNCTIONS 64
8.3.3 RATIONALE OF THE FUNCTION STRENGTH 67
8.3.4 ADEQUACY OF ASSURANCE MEASURES 68
8.4 PP CLAIMS RATIONALE 71

1 ST Security Target (ST) Overview

This chapter outlines the Security Target (ST); the ST identification information, ST overview, and gives information on the Common Criteria (CC) conformance, terminology, acronyms, and trade marks.

1.1 ST Identification

The identification information for this ST is as follows.

ST Title	SEIKO EPSON PP-100N Security control unit Security Target
ST Version	2.0
Publication Date	2009/07/03
Author	SEIKO EPSON CORPORATION
TOE Title	PP-100N Security control unit
TOE Version	1.00
Evaluation Assurance Level	EAL3
Keywords	Seiko Epson, Epson, CD-R, DVD-R, Publisher, Printer, Autoloader, Taking out, Electronic lock
CC Version	Common Criteria for Information Technology Security Evaluation Part1: Introduction and general model Version 2.3 August 2005 CCMB-2005-08-001 Part2: Security functional requirements Version 2.3 August 2005 CCMB-2005-08-002 Part3: Security assurance requirements Version 2.3 August 2005 CCMB-2005-08-003

1.2 ST Overview

The ST describes the specifications of the TOE; PP-100N Security control unit. The PP-100N is a disc publisher which writes electronic information acquired over a network on discs such as CD-Rs or DVD-Rs and prints images on the discs. The TOE provides the following security functions in order to let the users to securely receive the discs they created.

- Identify Authentication function
- Controlled Distribution function
- Electronic Lock Open function
- Warning function
- Setting Data Control function

1.3 CC Conformance

This ST conforms to the following standards;

- Functional requirements: CC Part 2 Extended
- Assurance requirements: CC Part 3
- Evaluation Assurance Level: EAL3
- There is no PP to be conformed.

1.4 Terminology and Acronyms

The table below explains the terms and acronyms used in this ST.

Table 1: Glossary

Term	Description
Disc	Disc-shaped storage medium such as a CD-R and DVD-R
Recording surface	The disc surface on which electric information is written.
Label surface	The printable side of the disc.
Blank disc	A disc that stores no data.
Published disc	A disc to/on which electronic information has been written and an image has been printed. Includes an error disc.
Error disc	A disc which the PP-100N failed to write electronic information to it or print on the label surface.
Label data file	A print data file to be printed on the label surface of the disc.
Disc image file	A data file to be recorded on the recording surface of the disc.
Spool data	Disc image files or label data files temporarily stored on the hard disc of PP-100N until they are recorded or printed on discs.
Operation log	The product operation history logged to be used for maintenance and support by service person.
Inspection log	Security-related log such as success and failure history of the security functions and access record to TSF data.
Source data	Source data of the disc image files
Stacker	A container that stacks discs to stores them.
Stacker 1	A detachable stacker for loading blank discs. In Security Mode, this is used to temporarily store discs.
Stacker 2	A detachable stacker to store published discs.
Stacker 3	A stacker to store published discs. Mounted on Stacker 4. This is not used in Security Mode.
Stacker 4	A stacker to store published discs that should be ejected by the pre-approved user.
Printer	An apparatus to print images on the label surface of discs.
Printer tray	A tray to put a disc to print on its label surface.

Drive	A disc drive to write a disc image file on the recording surface of a disc. PP-100N is equipped with two disc drives.
Control panel	User interface consists of LCD, LED, and operation buttons.
Disc cover	A cover on the front of PP-100N. Usually, it is locked physically or electronically by the disc cover lock and can be opened by deactivating the lock. When it opens, the user can access the following. - Stacker 1 - Stacker 2 - Drive - Printer - Security lock switch
Job	A disc publishing work unit of PP-100N.
Job ID	A number used to identify each job.
SMTP server	A mail server used to notify the user of a PP-100N status.
Security mode	PP-100N offers two modes; Security mode and non-security mode. In the Security mode, the following functions indispensable for the security work. - Identify Authentication function - Controlled Distribution function - Electronic Lock Open function - Warning function - Setting Data Control function This ST describes the specifications of the Security mode.
PP-100N Web application	Web applications that can be activated from a client PC using the web server function preinstalled on PP-100N. They are used to request for approval of publishing discs, to approve the request, and to register/change the setting and user information.
Total Disc Maker	An application that is installed on a client PC. This allows the user to select files to be written to discs and to create label print data.
Total Disc Monitor	An application that is installed on a client PC. This allows the user to check a job status, pause/resume a job, and cancel a job.
Total Disc Setup	An application that is installed on a client PC. This allows the user to make an initial setup of Total Disc Maker.
Security pack	These are needed to use PP-100N in the Security mode. - PP-100N Security Administrator's Guide - PP-100N Security User’s Guide - PP-100N security activation key sheet

Any other acronyms explained in CC Part1 are omitted.

1.5 Trademarks

All company names and product names are trademarks or registered trademarks of their respective companies.

2 TOE Description

This chapter describes the TOE overview, parties involved with TOE, physical configuration, logical configuration, protected assets, and TOE functions.

2.1 TOE Overview

2.1.1 Type of Product

The TOE is a security control unit embedded in PP-100N, which is a CD-R/DVD-R publisher, and consists of the following security control software and hardware.

- Identify Authentication [Web_app] function: identifies and authenticates the user who logs into PP-100N through PP-100N Web application.
- Identify Authentication [Cli_app] function: identifies and authenticates the user who logs into PP-100N through Total Disc Maker or Total Disc Monitor.
- Identify Authentication [Panel] function: identifies and authenticates the user who logs into PP-100N using its control panel.
- Controlled Distribution function: ejects published discs only for the user who created them.
- Electronic Lock Open function: allows only administrator to deactivate the electronic lock of the disc cover.
- Warning function: warns the administrator if a possibility of security problem is detected.
- Setting Data Control function: allows only authorized users to access the information required to manage PP-100N such as the settings control and job information.

2.1.2 Intended Use

The TOE is intended to restrict access to published discs to the user who created them. This protects the published discs from falling into the hands of anyone except the user and prevents leakage of data recorded on them.

2.1.3 Environment of Use

The following figure shows a typical environment in which this TOE is used.

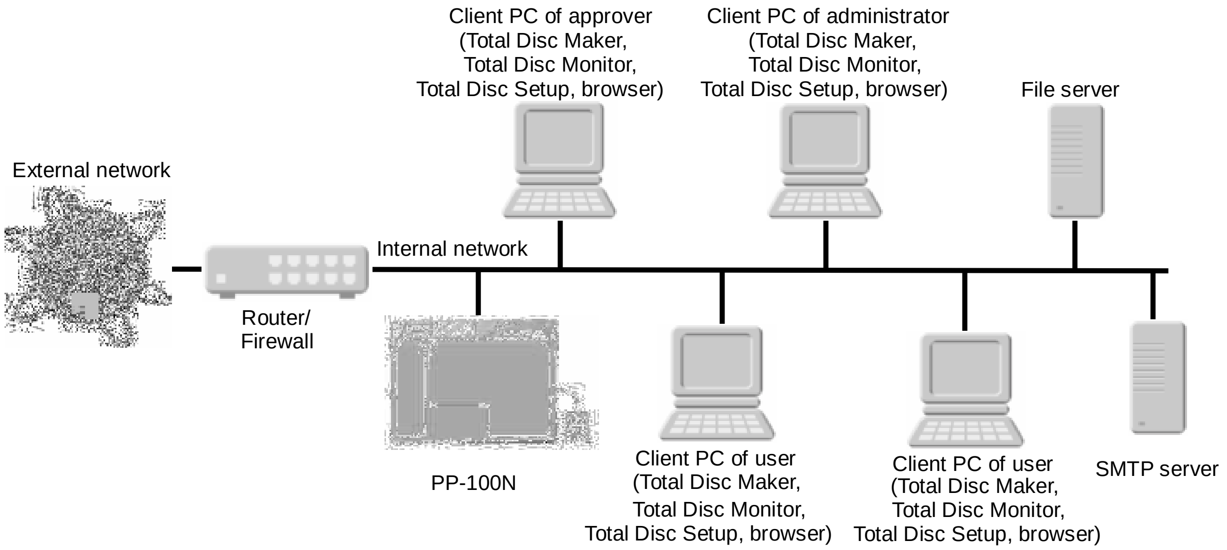

Figure 1: Environment of Use

PP-100N is often installed in an office room where customer information is handled. It is connected to the internal network and the network is connected to external network secured by a router and a firewall. To the internal network, client PCs, SMTP server, file server, and etc. are also connected. On the client PC of the user who creates discs, Total Disc Maker, Total Disc Monitor, Total Disc Setup, and a browser are installed. There may be an environment which do not use external network, SMTP server, and file server, however, the lack of them makes no difference to the TOE features.

2.2 Parties involved with TOE

The following table lists the parties/persons involved with this TOE.

Table 2: Parties involved with TOE

Party	Role & Privilege	Knowledge & Level of trust
Responsible of the organization	A responsible person in the office in where PP-100N installed. This person appoints an administrator and approver.	Reliable person who never try malicious attempts against TOE operations.
Users	Office persons who are allowed to publish discs using PP-100N. In other words, a collective term for the administrator, approver, and the person in charge of publishing discs.	
Administrator	A person who manage the usage of PP-100N.	Reliable person who never try malicious attempts against TOE operations.
Publisher (person in charge of publishing discs)	Users other than the administrator and approver.	Not always be trusted. There is a possibility that the person will try malicious attempts against TOE operations. Not an information processing specialist.
Approver	A person authorized to approve disc publishing application submitted by persons in charge of the job.	Reliable person who never try malicious attempts against TOE operations.
Service person	SEIKO EPSON company member, overseas subsidiary company member, or service contractor member who takes charge in repairing and maintaining PP-100N.	Not always be trusted. There is a possibility that the service person will try malicious attempts against TOE operations. He/She has know-how on repairing PP-100N, but is not an information processing specialist.
Third party	Any persons other than above.	There is a possibility that the person will try malicious attempts against TOE operations. Not an information processing specialist.

2.3 Physical Configuration

2.3.1 Hardware Configuration

The following figure shows the hardware configuration in which this TOE is used. The yellow boxes indicate the components included in this TOE.

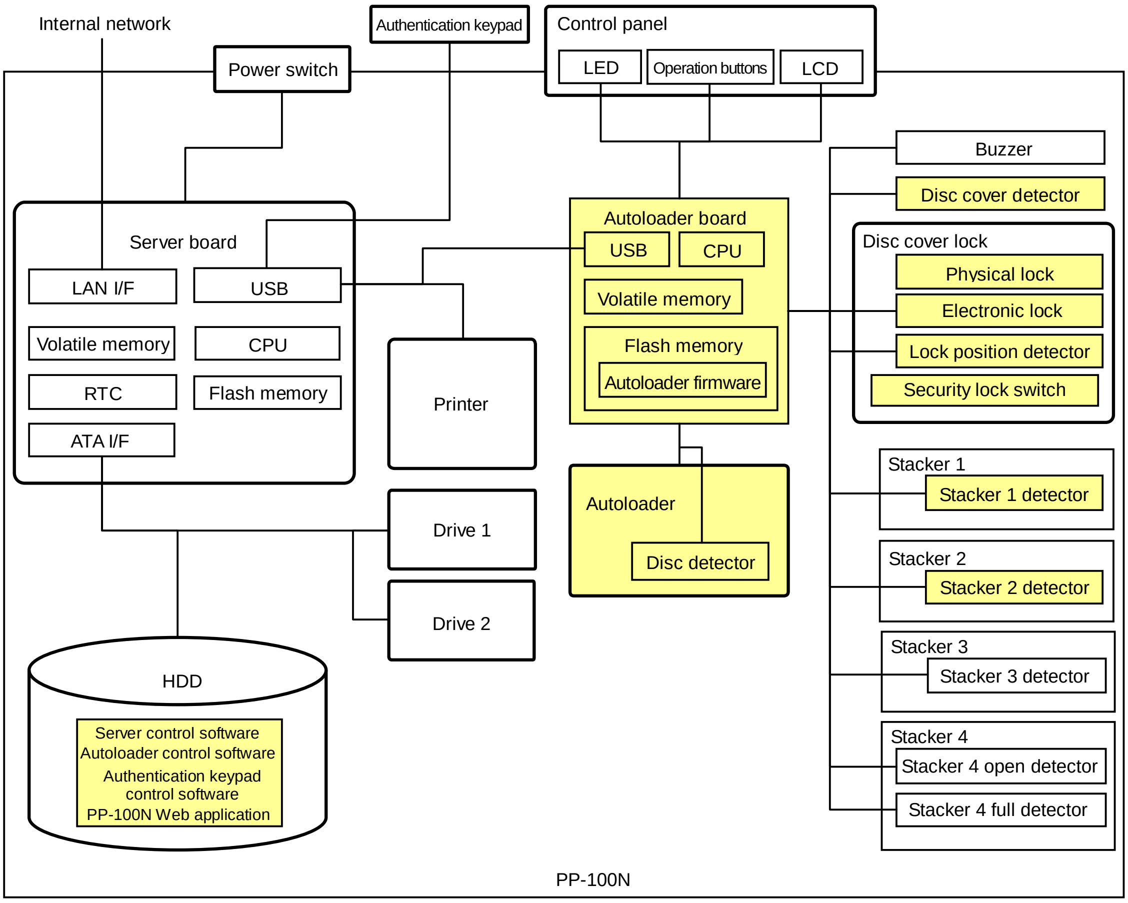

Figure 2: Hardware Configuration

2.3.2 Hardware Components

The table below explains the hardware components.

Table 3: Hardware Components

Component	Description
Autoloader board	A CPU board consists of flash memory in which autoloader firmware embedded, input/output port and such, and controls the following. - Autoloader - Disc detector - Control panel - Buzzer - Disc cover detector - Electronic lock

	- Lock position detector - Stacker 1 detector - Stacker 2 detector - Stacker 3 detector - Stacker 4 open detector - Stacker 4 full detector
Autoloader	A device to transfer the discs to a requested location (Stacker 1, Stacker 2, Stacker 4, printer tray or drive).
Disc detector	A detector to detect whether the autoloader is holding the discs or not. This is also used to check the remaining discs in Stacker 1 and 2.
Server board	A CPU board that makes total control over PP-100N. The followings are mounted on the board; CPU, memory, LAN I/F, USB I/F (to control the autoloader, printer and authentication keypad), ATA I/F (to control the built-in hard disc drive and drives), an encrypting chip (to encrypt the data in RTC and hard disc drive).
HDD	A hard disc drive for the server board. Server control software and PP-100N Web application are preinstalled on the drive. It also records spool data and setting control data.
Disc cover detector	A detector to detect opening/closing status of the disc cover.
Disc cover lock	A lock for the disc cover. There are two types of lock; electronic key that can be activated/deactivated using software and physical key. Using either one of the two, the disc cover can be opened. The disc cover is automatically locked as soon as it is closed.
Electronic lock	A lock which can be deactivated electronically by the software control.
Physical lock	A lock which can be opened using a physical key.
Lock position detector	A detector to detect opening/closing of the disc cover lock and on/off of the security lock switch.
Security lock switch	A switch to turn the disc cover lock function on or off. When it is off, the disc cover is kept unlocked all the time, and if it is on, the disc cover lock is activated.
Stacker 1 detector	A detector to detect removing/reattaching status of a stacker from/to Stacker 1.
Stacker 2 detector	A detector to detect removing/reattaching status of a stacker from/to Stacker 2.
Stacker 3 detector	A detector to detect removing/reattaching status of Stacker 3.
Stacker 4 open detector	A detector to detect that Stacker 4 is pulled out.
Stacker 4 full detector	A detector to detect that Stacker 4 is full with discs.
Power switch	Power switch of PP-100N.
LCD	A display to show operation menu or warning messages.
LED	A light-emitting diode to show the status of PP-100N as follows. - POWER LED: shows power on/off, and printer cleaning status - BUSY LED: shows that disc publication (burning/printing) is in progress - ERROR LED: lights when an error occurs
Operation buttons	The buttons to operate the menu displayed on the LCD.
Buzzer	A device to notify the user with sounds in the event of a PP-100N failure.

Authentication keypad	A USB keypad used for identity authentication to operate PP-100N. This keypad is an optional and not included in the PP-100N kit, but necessary to operate TOE. This should be prepared and connected to PP-100N by the administrator.

2.3.3 Hardware of the TOE

The following shows the hardware components included in this TOE. (Refer to the yellow boxes in “Figure 2: Hardware Configuration”.)

- Autoloader board
- Autoloader
- Disc detector
- Disc cover detector
- Physical lock
- Electronic lock
- Lock position detector
- Security lock switch
- Stacker 1 detector
- Stacker 2 detector

2.3.4 Software Configuration

The following figure shows the software configuration in which this TOE is used. The yellow boxes indicate the functions included in this TOE.

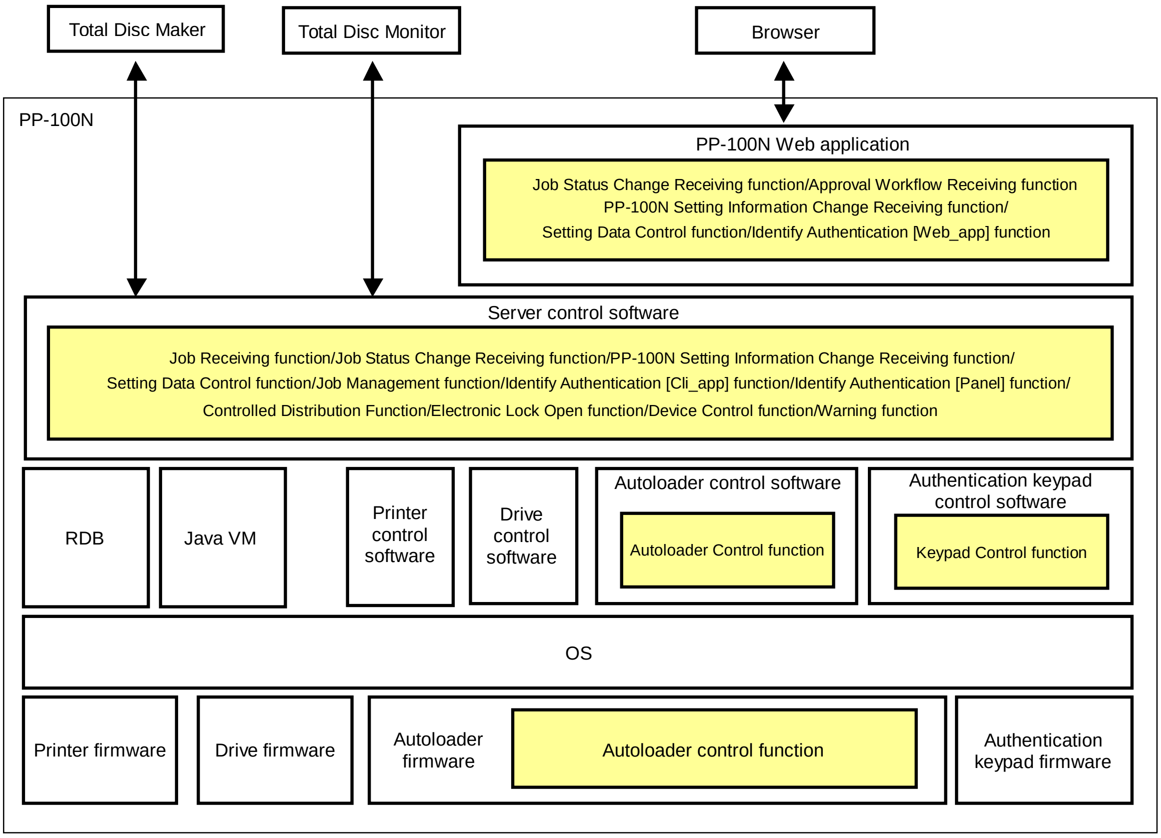
Total Disc Maker
Total Disc Monitor
Browser
PP-100N
PP-100N Web application
Job Status Change Receiving function/Approval Workflow Receiving function
PP-100N Setting Information Change Receiving function/
Setting Data Control function/Identify Authentication [Web_app] function
Server control software
Job Receiving function/Job Status Change Receiving function/PP-100N Setting Information Change Receiving function/
Setting Data Control function/Job Management function/Identify Authentication [Cli_app] function/Identify Authentication [Panel] function/
Controlled Distribution Function/Electronic Lock Open function/Device Control function/Warning function
RDB
Java VM
Printer control software
Drive control software
Autoloader control software
Autoloader Control function
Authentication keypad control software
Keypad Control function
OS
Printer firmware
Drive firmware
Autoloader firmware
Autoloader control function
Authentication keypad firmware

Figure 3: Software Configuration

2.3.5 Software Components

The table below explains the software components.

Table 4: Software Components

Component	Description
PP-100N Web application	Applications that can be activated from a client PC using the web server function preinstalled on PP-100N. They are used to request for approval of publishing discs, to approve the request, and to register/change the setting and user information.
Total Disc Maker	An application that is installed on a client PC. This allows the user to select files to be written to discs and to create label print data.
Total Disc Monitor	An application that is installed on a client PC. This allows the user to check a job status, pause/resume a job, and cancel a job.
Server control software	A software to make total control over PP-100N. It is embedded in the server board and runs under OS embedded in the board.
RDB	Relational database which handles the following. - Setting control data - Job information - Disc position information - Inspection log - Operation log - Spool data path (physical position information)
Autoloader control software	Library to control the autoloader.
Printer control software	Library to control the printer.
Drive control software	Library to control the drive.
Authentication keypad control software	Library to control the authentication keypad.
Printer firmware	A firmware mounted on the printer board to control the printer mechanism.
Drive firmware	A firmware mounted on the drive to control the drive mechanism.
Autoloader firmware	A firmware mounted on the autoloader board to control the following. - Autoloader - Control panel - Buzzer - Disc cover detector - Electronic lock - Lock position detector - Stacker 1 detector - Stacker 2 detector - Stacker 3 detector - Stacker 4 open detector - Stacker 4 full detector
Authentication keypad firmware	A firmware to control the authentication keypad.

Browser	An application to allow the users to browse web pages.
Java VM	A software to convert the Java bytecode into native code of the platform, and to execute it.

2.3.6 TOE Range of the Software

The TOE range of the software is part of the following softwares. (Refer to the yellow boxes in “Figure 3: Software Configuration”.)

- Server control software
- PP-100N Web application
- Autoloader control software
- Autoloader firmware
- Authentication keypad control software

2.4 Logical Configuration

2.4.1 Logical Configuration

The following figure shows the logical configuration of the TOE. The yellow box indicates the TOE logical range.

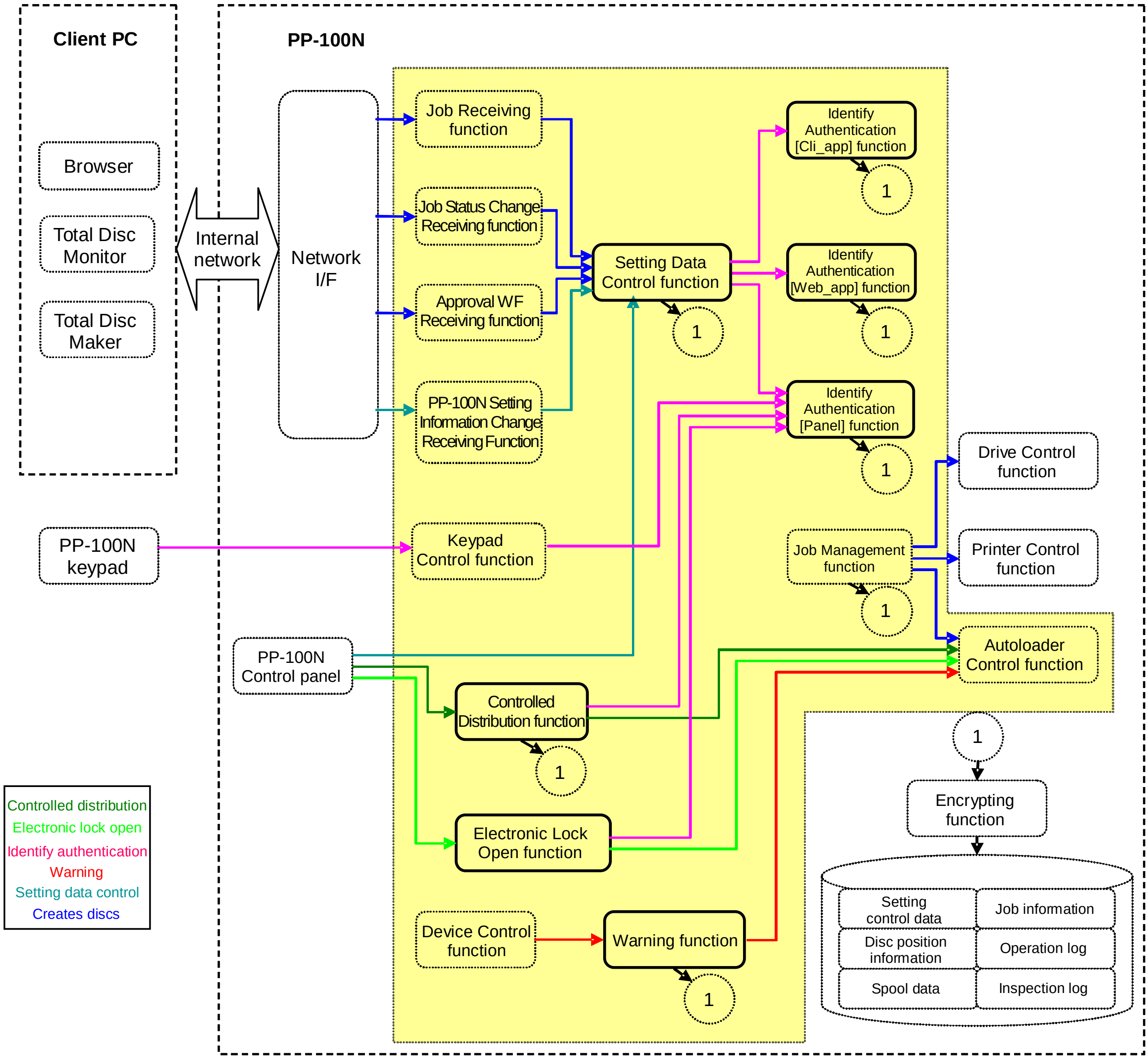

Figure 4: Logical Configuration

2.4.2 Logical Components

The table below explains the logical components.

Table 5: Logical Components

Component	Description
Identify Authentication [Panel] function	Identifies and authenticates the user who logs into PP-100N using its control panel to take out discs, deactivate the electronic lock or change the setting of PP-100N.
Identify Authentication [Web_app] function	Identifies and authenticates the user who logs into PP-100N through PP-100N Web application to operate the user information or setting information.
Identify Authentication [Cli_app] function	Identifies and authenticates the user who logs into PP-100N through Total Disc Maker or Total Disc Monitor to check a job status, pause, resume or cancel a job.
Controlled Distribution function	Controls the autoloader to move published discs only that which the user created from Stacker 2 to Stacker 4.
Electronic Lock Open function	Allows only administrator to deactivate the electronic lock of the disc cover.
Warning Function	Warns the administrator using the buzzer, LED and LCD if a security problem arises on PP-100N.
Setting Data Control function	Allows only authorized users to access the information required to manage PP-100N such as the settings control and job information.
Device Control function	Receives/requests information from/to disc cover detector, lock position detector, disc detector, Stacker 1 detector, Stacker 2 detector, Stacker 3 detector, Stacker 4 open detector and Stacker 4 full detector.
Drive Control function	Controls the drive.
Printer Control function	Controls the printer.
Autoloader Control function	Controls the autoloader.
Job Management function	Manages the job processing.
Job Receiving function	Receives the job.
Job Status Change Receiving function	Receives a request to change the job information.
Approval Workflow Receiving function	Receives information on disc publishing approval from the approver.
PP-100N Setting Information Change Receiving function	Receives a request to change the PP-100N setting.
Keypad Control function	Converts a signal entered using the keypad into a command for the server control software.
Encrypting function	Encrypts/decrypts the data to be stored on PP-100N hard disc drive.
Setting control data	A collective term for the PP-100N setting information and user information.

Job information	Various information related to each job.
Disc position information	Information about whether discs should be in Stacker 2 or not for each job.
Spool data	Disc image files or label data files temporarily stored on the hard disc of PP-100N until they are recorded or printed on discs.
Operation log	The product operation history logged to be used for maintenance and support by service person.
Inspection log	Security-related log such as success and failure history of the security functions and access record to TSF data.

2.4.3 Logical Scope and Boundary of the TOE

The following shows the logical scope and boundary of the TOE. (Refer to the yellow box in "Figure 4: Logical Configuration".)

- Identify Authentication [Web_app] function
- Identify Authentication [Cli_app] function
- Identify Authentication [Panel] function
- Controlled Distribution function
- Electronic Lock Open function
- Warning Function
- Setting Data Control function
- Device Control function
- Job Management function
- Autoloader Control function
- Job Receiving function
- Job Status Change Receiving function
- Approval Workflow Receiving function
- PP-100N Setting Information Change Receiving function
- Keypad Control function

2.5 Protected Assets

The assets protected by this TOE are data in published discs stored in PP-100N. Confidential information of the PP-100N owner company has been written to the discs. If anyone can take out the discs from PP-100N, it is easy for he or she who took out the discs to see the contents. No special information processing knowledge is required. The published discs must be taken out precisely by the user approved to create the discs.

The following explains the data asset movement during the disc publishing.

1. The user selects source files on a file server or the client PC, and creates a disc image file on the client PC. Because the source files and disc image file exist on the file server or PCs managed by the company, those files are not assets protected by this TOE.
2. The disc image file is sent to PP-100N and stored as spool data on PP-100N hard disc drive.

3. The spool data is written to discs when the user operated to do so, and the discs are stored in PP-100N. The disc cover that must be opened to take out the discs is locked so that unauthorized opening attempts can not be achieved.
4. The discs are ejected to Stacker 4 upon the request from the created user.
5. Once the discs are taken out by the user who created them, the user is responsible for securely storing the discs, therefore the ejected discs are not asset protected by this TOE.

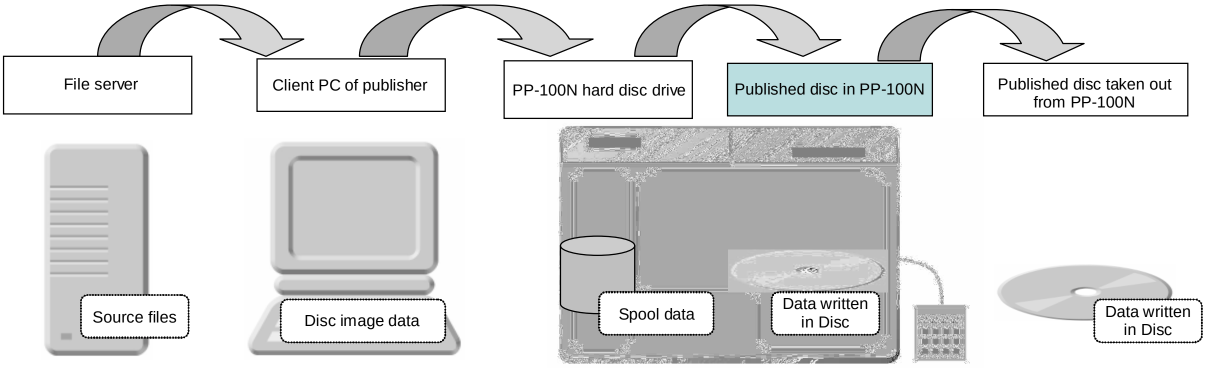

Figure 5: Data Asset Movement

Data asset that must be protected by this TOE is defined as follows; data in discs from when a spool data is written to the discs until they are ejected to Stacker 4.

2.6 TOE Functionality

2.6.1 TOE Functions

Security Functions offered by TOE

- Identify Authentication function
  - Identify Authentication [Web_app] function

    This function identifies and authenticates the user who logs into PP-100N through PP-100N Web application via a browser on a client PC.
  - Identify Authentication [Cli_app] function

    This function identifies and authenticates the user who logs into PP-100N through Total Disc Maker or Total Disc Monitor on a client PC.
  - Identify Authentication [Panel] function

    This function identifies and authenticates the user who logs into PP-100N using its control panel.

- Controlled Distribution function

This function is to eject published discs stored in Stacker 2 to Stacker 4. When the EJECT button on the PP-100N control panel is pressed, the Controlled Distribution function activates the Identify Authentication [Panel] function to identify the user. Then, the Controlled Distribution function checks if the discs published by the user who identified by the Identify Authentication [Panel] function exist in Stacker 2 or not, and if they exist, controls the autoloader to transfer the discs to Stacker 4.

- ■ Electronic Lock Open function

This function deactivates the electronic lock of the disc cover. When the menu for deactivating the electronic lock on the control panel of PP-100N is selected, the Electronic Lock Open function activates the Identify Authentication [Panel] function to identify the user. If the user is identified as the administrator by the function, the electronic lock is deactivated.

- ■ Warning Function

This function warns the administrator using the following methods whenever the possibility of security problem is detected.

- Sounds a buzzer
- Turns on the ERROR LED
- Displays security warning information on the LCD

The following shows the possibilities of security problems.

1) Published discs exist in PP-100N

- The published discs exist in PP-100N during the power-off process.

2) The disc cover is not locked

- The disc cover is kept open for 60 seconds or more.
- The disc cover is not physically locked for 10 seconds or more after the cover is closed.
- The security lock switch is off for 10 seconds or more after the cover is closed.

3) Drops a disc

- The autoloader drops a disc

4) Removing Stacker 2

- “Stacker 2 is removed and attached while the disc cover is open”, and “the discs exist in Stacker 2 when the disc cover is closed”.

- ■ Setting Data Control function

This function restricts the following operations to the users identified and authenticated by Identify Authentication [Web_app] function, Identify Authentication [Cli_app] function and Identify Authentication [Panel] function; access to the setting control data or job information, browsing, adding, changing or deleting the setting control data or job information.

Non-security Functions offered by TOE

- ■ Device Control function

This function receives/requests information from/to Disc cover detector, Lock position detector, Disc detector, Stacker 1 detector, Stacker 2 detector, Stacker 3 detector, Stacker 4 open detector and Stacker 4 full detector.

- ■ Job Management function

This function manages the job processing. Monitors the job information and when the job status is changed, executes the next process of the job or next job.

■ Autoloader Control function

This function controls the autoloader to transfer the discs to requested location (Stacker 1, Stacker 2, Stacker 4, printer tray or drive).

■ Job Receiving function

This function receives jobs issued by Total Disc Maker.

■ Job Status Change Receiving function

This function receives requests from Total Disc Monitor for checking the job processing status, pausing, resuming or cancelling jobs, and also receives job approval application from PP-100N Web application.

■ Approval Workflow Receiving function

This function receives information on disc publishing approval from the approver.

■ PP-100N Setting Information Change Receiving function

This function receives requests to change PP-100N setting from administrator.

■ Keypad Control function

This function converts a signal entered using keypad into a command for the server control software.

2.6.2 Usage

The following figure shows a flow for publishing discs.

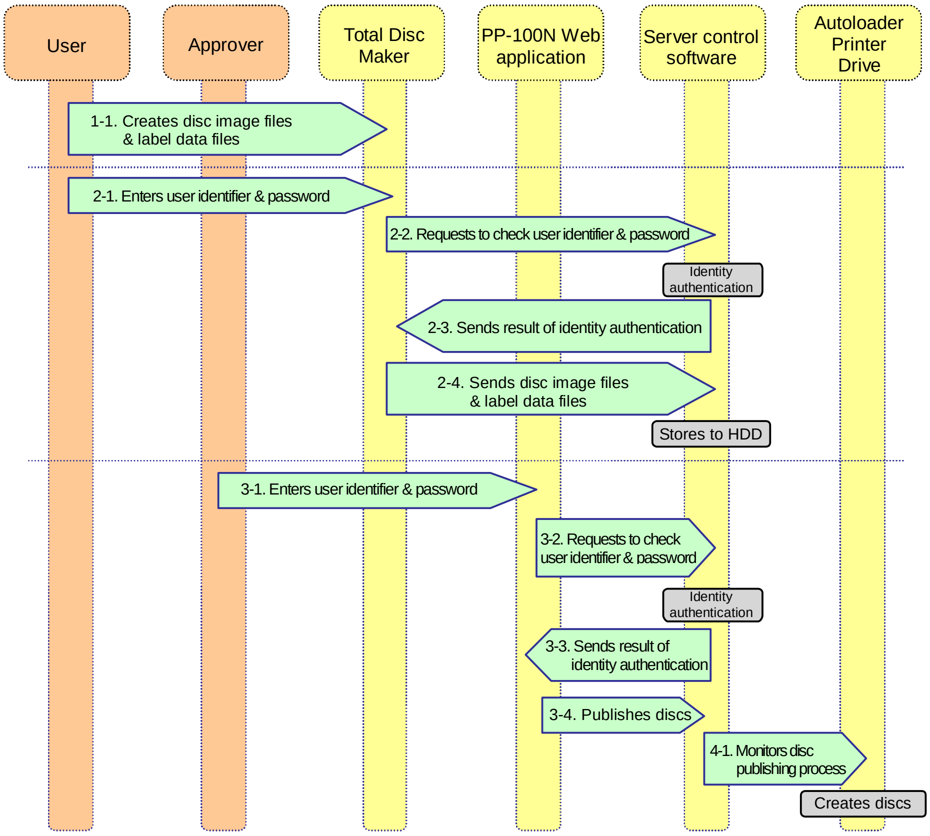
User
Approver
Total Disc Maker
PP-100N Web application
Server control software
Autoloader Printer Drive
1-1. Creates disc image files & label data files
2-1. Enters user identifier & password
2-2. Requests to check user identifier & password
Identity authentication
2-3. Sends result of identity authentication
2-4. Sends disc image files & label data files
Stores to HDD
3-1. Enters user identifier & password
3-2. Requests to check user identifier & password
Identity authentication
3-3. Sends result of identity authentication
3-4. Publishes discs
4-1. Monitors disc publishing process
Creates discs

Figure 6: Publishing Discs

1 Creating disc image files

1. The user selects source files on a file server or the client PC, and creates disc image files and label data files using Total Disc Maker on the client PC.

2 Sending the disc image files

1. The user performs disc publishing on Total Disc Maker, and enters his/her user identifier [Appli] and password [Appli].
2. Total Disc Maker requests the server control software to check if the user is authenticated.
3. The server control software executes identity authentication and sends the result to Total Disc Maker.
4. Total Disc Maker sends the disc image files and label data files to PP-100N. They are stored as spool data on PP-100N hard disc drive.

3 Disc approval

1. The approver starts the PP-100N Web application, and enters his/her user identifier [Appli] and password [Appli].
2. The PP-100N Web application requests the server control software to check if the user is authenticated.
3. The server control software executes identity authentication and sends the result to the PP-100N Web application.
4. The PP-100N Web application sends out a command to the server control software to publish the discs.

4 Publishing the discs

1. The server control software monitors job information and when the software detects that the job is ready for publishing discs, it executes the publishing process (writing data, label printing). The published discs are stored in Stacker 2.

The following figure shows a flow of job operation and taking out the discs.

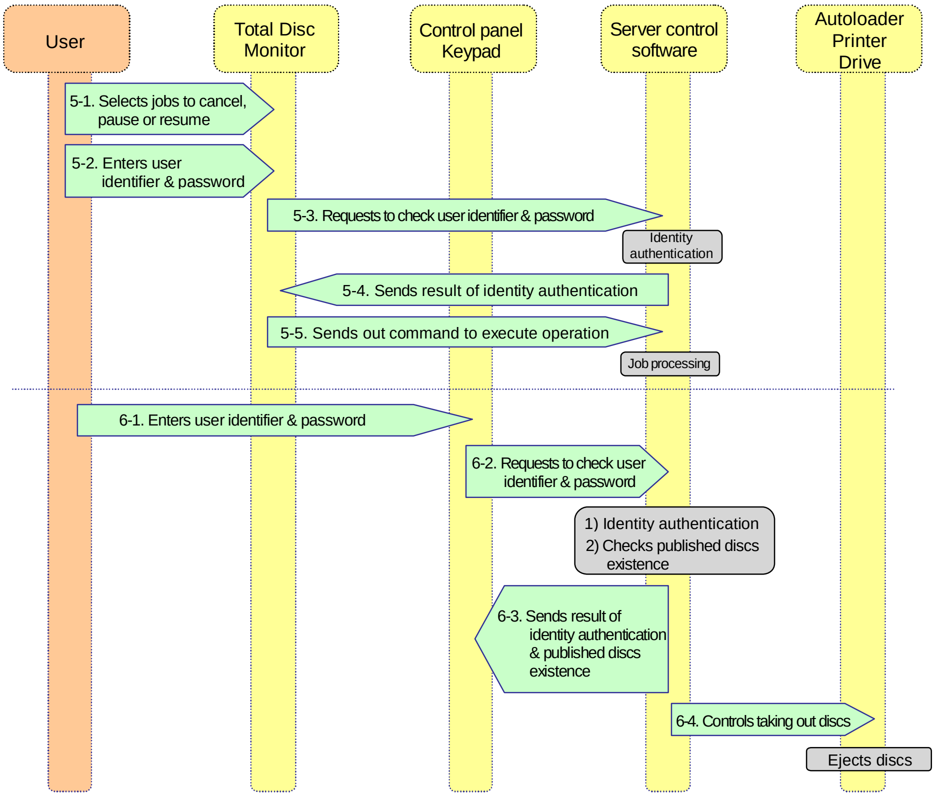
User
Total Disc Monitor
Control panel Keypad
Server control software
Autoloader Printer Drive
5-1. Selects jobs to cancel, pause or resume
5-2. Enters user identifier & password
5-3. Requests to check user identifier & password
Identity authentication
5-4. Sends result of identity authentication
5-5. Sends out command to execute operation
Job processing
6-1. Enters user identifier & password
6-2. Requests to check user identifier & password
1) Identity authentication
2) Checks published discs existence
6-3. Sends result of identity authentication & published discs existence
6-4. Controls taking out discs
Ejects discs

Figure 7: Job Operation and Taking Out the Discs

5 Job operation

1. The user selects pausing, resuming, or cancelling a job on Total Disc Monitor. The available jobs are “approved” jobs that are “waiting for publishing discs” or jobs whose “publishing discs" process is in progress. Depending on which operation is requested from the user, the available jobs differ as follows.
   - Pausing

   Jobs whose status is “approved” and “waiting for publishing discs” or “publishing discs".
   - Resuming

   Jobs whose status is “pausing”.
   - Cancelling

   Jobs whose status is “approved” and “waiting for publishing discs” or “publishing discs".
   Jobs whose status is “pausing”.
2. The user enters his/her user identifier [Appli] and password [Appli] on Total Disc Monitor.
3. Total Disc Monitor requests the server control software to check if the user is authenticated.
4. The server control software executes identity authentication and sends the result to Total Disc Monitor.
5. Total Disc Monitor sends out a command to the server control software to execute the requested operation.

6 Taking out discs

1. The user who published discs presses the EJECT button on the PP-100N control panel, and enters his/her user identifier [Panel] and password [Panel] using the authentication keypad.
2. The server control software is requested to check if the user is authenticated and whether any discs published by the user exist or not.
3. The server control software executes identity authentication and checks the discs existence, and sends the results.
4. The server control software controls the autoloader to transfer the discs published by the authorized user from Stacker 2 to Stacker 4.

2.6.3 Operational Procedure

The users must follow the operational procedures below to make TOE operate properly.

<Before starting operation>

The administrator must finish the following preparations for the TOE before using PP-100N with a Security pack.

1. Connect the authentication keypad to PP-100N.

Connect the authentication keypad to the USB port inside PP-100N.

2. Make security mode setup

The menu is displayed on the control panel when PP-100N is turned on. Follow the menu to set security mode.

3. Make network setup

Make network setup such as IP address setting using the menu on the control panel.

4. Install the application on a client PC

Using the bundled install CD, install Total Disc Maker, Total Disc Setup and Total Disc Monitor on the client PC.

5. Register PP-100N

Start Total Disc Setup on the client PC, and register PP-100N.

6. Register an administrator

Start the browser on the client PC and directly access to PP-100N. When accessing, register the administrator.

7. User information management

Start the PP-100N Web application, and register the user information after the administrator is identified and authenticated by identifier [Appli] and password [Appli].

8. Check the TOE version

Using the menu on the control panel, check the TOE version.

<When using PP-100N in Security Mode>

The administrator is required the following in security mode.

1. User information management

Start the PP-100N Web application, and register/change the user information after the administrator is identified and authenticated by identifier [Appli] and password [Appli].

2. Load blank discs

Display the menu on the control panel and enter user identifier and password using the authentication keypad. After identified/authenticated, open the disc cover and load blank discs in Stacker 1.

3. When turning the power on

When turning the power on, take out all discs from Stacker 2.

4. When removing Stacker 2.

When removing Stacker 2, take out all discs from Stacker 2.

5. When an alert is issued

If a security problem arises for PP-100N and alerted, remove the cause immediately.

The users are required to perform the following operation.

1. Self-information management

Start the PP-100N Web application, and change the user’s own password [Appli] and password [Panel] after the user is identified and authenticated by identifier [Appli] and password [Appli].

<Maintenance and repair>

In the case of PP-100N failure, the user can send the PP-100N to the PP-100N service center (off-site service), or call a service person (on-site service). Depending on which service is used, the administrator should perform as follows.

1. On-site service

While the service person is servicing PP-100N, the administrator should be there to watch the servicing work.

2. Off-site service

The administrator should remove the published discs from PP-100N and delete all setting control data before sending the product to the service center.

2.7 Evaluation Configuration

The following shows evaluation configuration used to test the TOE.

- OS of the client PC

    Windows XP Professional SP3

    Windows Vista Ultimate SP1

- Browser

    Internet Explorer6 SP3

    Internet Explorer7

- Client application

    Total Disc Monitor Ver.2.0

    Total Disc Maker Ver.2.0

- Keypad

    SANWA SUPPLY NT-9UBK

3 TOE Security Environment

This chapter describes the security environment for the TOE; the assumptions, threats, and organizational security policies.

3.1 Assumptions

The assumptions are as follows.

A.Approver

An approver is a reliable person who never tries malicious attempts against TOE operations.

A.Administrator

An administrator is a reliable person who never tries malicious attempts against TOE operations.

A.Password

The user password is not leaked to anyone except the user. The password is not easily guessed and changed on a regular basis.

A.Operation status management

The administrator monitors the PP-100N's operation status to prevent the followings from occurring.

- Destroying PP-100N
- Unlocking of the disc cover by anyone except the administrator

A.Security mode

The administrator connects the authentication keypad to PP-100N included in the security pack, and makes security mode setup for the PP-100N.

A.Network

The network environment satisfies the following requirements.

- TOE is not subjected to attacks from external networks.
- The internal network where the TOE devices are connected is protected from being bugged.

3.2 Threats

The possible threats are as follows.

T.Taking out of discs

Anyone except the user who published the discs may pretend to be the user or the administrator, and take out published discs and leak the disc data.

T.Disc cover unlocked

When the disc cover is unlocked by the mistake of the administrator, anyone except the user who published the discs may take out the discs and leak the disc data.

T.Dropping of discs

When the autoloader drops published discs during transferring, the published discs may go into Stacker 4. In such case, anyone except the user who published the discs may take out the discs and leak the disc data.

T.Misplacement of discs

When published discs is ejected due to the disc misplacement to Stacker 2 by the administrator or the service person, anyone except the user who published the discs may take out the discs and leak the disc data.

3.3 Organizational Security Policies

The organizational security policies are as follows.

P.Published discs

PP-100N is not stopped with published discs remained inside it.

4 Security Objectives

This chapter describes the security objectives; the security objectives for the TOE and for the environment.

4.1 Security Objectives for the TOE

The security objectives for the TOE are as follows.

O.Identify Authentication

The TOE shall identify and authenticate the user who accesses to the TOE while keeping the password [Panel] of the user secret.

O.Controlled Distribution

The TOE shall take out only the discs published by the user.

O.Cover open restriction

The TOE shall allow only the administrator to deactivate the electronic lock of the disc cover.

O.Registration

The TOE shall allow only the administrator to add, change, delete, or consult the user information (except consulting of password [Appli], password [Panel]), and change or consult the setting information. The TOE shall allow each user to change his/her own password [Appli] and password [Panel].

O.Warning

The TOE shall detect the following statuses that show the possibility of security problem and warn the administrator if any of them is detected.

- Published discs are detected inside the PP-100N during a power-off process.
- The disc cover is left unlocked.
- The autoloader dropped discs.
- During the PP-100N is powered, discs are detected in Stacker 2 after the stacker is removed and reattached.

4.2 Security Objectives for the Environment

The security objectives for the TOE are as follows.

OE.Reliability of approver

A responsible of the organization shall appoint a reliable person as the approver.

OE.Reliability of administrator

A responsible of the organization shall appoint reliable persons as the administrators and educate them.

OE.Handling by administrator

The administrator shall take a prompt action against a TOE security problem arose while PP-100N is used or maintained.

OE.Password management

The user shall set his/her own password properly and change it according to the TOE Guidance document, and keep the password secret from anyone else.

OE.Monitoring by administrator

The administrator shall monitor PP-100N operation status to prevent the followings from occurring.

- Destroying PP-100N
- Unlocking of the disc cover by anyone except the administrator

OE.Security mode setting

Before using PP-100N, the administrator shall purchase the security pack and make the following setup.

- Connects the authentication keypad to the PP-100N
- Sets security mode on the PP-100N

OE.Network

The administrator shall take measures against intrusion from external network, and protect the internal network from being bugged.

OI.Password security

The Total Disc Maker and Total Disc Monitor shall perform user authentication while keeping the user password [Panel] secret.

5 IT Security Requirements

This chapter describes the IT security requirements; the security requirements for the TOE and for the IT environment.

5.1 TOE Security Requirements

This section describes the TOE security requirements; the TOE security functional requirements, the TOE security assurance requirements, and the minimum strength of function.

5.1.1 TOE Security Functional Requirements

The TOE security functional requirements are as follows. This ST newly creates and uses TOE Security Functional Requirements (FAU_GET.1 Event log acquisition).

FAU_ARP.1 Security alarm

Hierarchical to: No other components.

FAU_ARP.1.1	The TSF shall enforce [assignment: list of actions to minimize the confusion] if a security problem is detected. [Assignment: list of actions to minimize the confusion] - Warns (sounds a buzzer, turns on the LED, displays a warning on the LCD)

Dependencies: FAU_SAA.1 Security problems possibility analysis

FAU_SAA.1 Security problems possibility analysis

Hierarchical to: No other components.

FAU_SAA.1.1	The TSF shall apply a set of rules for monitoring target events, and based on the rules, the TSF shall be able to indicate the possibilities of TSP problems.
FAU_SAA.1.2	The TSF shall enforce the following rules for monitoring target events. a) Collects all or combines [assignment: subset defined as target events to be monitored] which are known as events that indicate the possibility of security problems. b) [Assignment: other rules] [Assignment: subset defined as target events to be monitored] - Published discs are detected inside the PP-100N during a power-off process. - The disc cover is left unlocked. - The autoloader dropped discs. - During the PP-100N is powered, discs are detected in Stacker 2 after the stacker is removed and reattached. [Assignment: other rules] None

Dependencies: FAU_GEN.1 Creating monitor data

FAU_GET.1 Event log acquisition

FAU_GET.1 acquires information on the target events.

Management: FAU_GET.1

There are no management activities foreseen.

Monitor: FAU_GET.1

There are no target events foreseen.

Hierarchical to: No other components.

FAU_GET.1.1	The TSF shall be able to acquire the event information on [assignment: individually defined events to be monitored]. [Assignment: individually defined events to be monitored] - Published discs are detected inside the PP-100N during a power-off process. - The disc cover is left unlocked. - The autoloader dropped discs. - During the PP-100N is powered, discs are detected in Stacker 2 after the stacker is removed and reattached.

Dependencies: No dependencies.

FIA_UAU.2[Panel] User authentication before any action

Hierarchical to: FIA_UAU.1

FIA_UAU.2.1	The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

Dependencies: FIA_UID.1 Timing of identification

FIA_UID.2[Panel] User identification before any action

Hierarchical to: FIA_UID.1

FIA_UID.2.1	The TSF shall require each user to identify itself before allowing any other TSF-mediated actions on behalf of that user.

Dependencies: No dependencies.

FIA_UAU.7[Panel] Protected authentication feedback

Hierarchical to: No other components.

FIA_UAU.7.1	The TSF shall provide only [assignment: list of feedback] to the user while the authentication is in progress. [Assignment: list of feedback] The same number of asterisks (*) as the entered characters.

Dependencies: FIA_UAU.1 Timing of authentication

FIA_AFL.1[Panel] Authentication failure handling

Hierarchical to: No other components.

FIA_AFL.1.1	According to the [assignment: list of authentication events], the TSF shall detect unsuccessful authentication attempts performed the number of times defined as follows; [selection: [assignment: positive integer number], an administrator configurable positive integer within [assignment: range of acceptable values]]. [Assignment: list of authentication events] User authentication of the server control software requested from the control panel [Selection: [assignment: positive integer number], an administrator configurable positive integer within [assignment: range of acceptable values]] [Assignment: positive integer number] 3
FIA_AFL.1.2	When unsuccessful authentication is attempted the defined number of times or more, the TSF shall enforce [assignment: list of actions]. [Assignment: list of actions] - Locks the user account for a predetermined time period (six hours for an administrator, one hour for others)

Dependencies: FIA_UAU.1 Timing of authentication

FIA_SOS.1[Panel] Verification of secrets

Hierarchical to: No other components.

FIA_SOS.1.1	The TSF shall provide a mechanism to verify that each password satisfies [assignment: a defined quality metric]. [Assignment: a defined quality metric] Password [Panel]: five or more numeric characters

Dependencies: No dependencies.

FIA_UAU.2[Appli] User authentication before any action

Hierarchical to: FIA_UAU.1

FIA_UAU.2.1	The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

Dependencies: FIA_UID.1 Timing of identification

FIA_UID.2[Appli] User identification before any action

Hierarchical to: FIA_UID.1

FIA_UID.2.1	The TSF shall require each user to identify itself before allowing any other TSF-mediated actions on behalf of that user.

Dependencies: No dependencies.

FIA_AFL.1[Appli] Authentication failure handling

Hierarchical to: No other components.

FIA_AFL.1.1	According to the [assignment: list of authentication events], the TSF shall detect unsuccessful authentication attempts performed the number of times defined as follows; [selection: [assignment: positive integer number], an administrator configurable positive integer within [assignment: range of acceptable values]]. [Assignment: list of authentication events] - User authentication of the server control software from the PP-100N Web application - User authentication of the server control software from Total Disc Maker - User authentication of the server control software from Total Disc Monitor [Selection: [assignment: positive integer number], an administrator configurable positive integer within [assignment: range of acceptable values]] [Assignment: positive integer number] 3
FIA_AFL.1.2	When unsuccessful authentication is attempted the defined number of times or more, the TSF shall enforce [assignment: list of actions]. [Assignment: list of actions] - Locks the user account for a predetermined time period (six hours for an administrator, one hour for others)

Dependencies: FIA_UAU.1 Timing of authentication

FIA_SOS.1[Appli] Verification of secrets

Hierarchical to: No other components.

FIA_SOS.1.1	The TSF shall provide a mechanism to verify that each password satisfies [assignment: a defined quality metric]. [Assignment: a defined quality metric] Password [Appli]: five or more alphanumeric characters or special characters (“.”, “–“, “_”)

Dependencies: No dependencies.

FDP_ETC.1 Exporting user data with no security attribute

Hierarchical to: No other components.

FDP_ETC.1.1	The TSF shall enforce [assignment: access control SFP(s) and/or information flow control SFP(s)] when exporting the user data, which is under control of the SFP(s), to outside of TSC. [Assignment: access control SFP(s) and/or information flow control SFP(s)] Controlled Distribution SFP
FDP_ETC.1.2	The TSF shall export user data without the security attribute related to the user.

Dependencies: [FDP_ACC.1 Subset access control or FDP_IFC.1 Subset information flow control]

FDP_ACC.1[Disk_eject] Subset access control

Hierarchical to: No other components.

FDP_ACC.1.1	The TSF shall enforce the [assignment: access control SFP] on [assignment: list of subjects, objects, and operations among subjects and objects covered by the SFP]. [Assignment: list of subjects, objects, and operations among subjects and objects covered by the SFP] Subject: - Process of the user who creates discs Object: - Job information - Disc position information Operations among subjects and objects covered by the SFP: - Checks and changes the job information - Checks, changes, deletes the disc position information [Assignment: access control SFP] Controlled Distribution SFP

Dependencies: FDP_ACF.1 Security attribute based access control

FDP_ACF.1[Disk_eject] Security attribute based access control

Hierarchical to: No other components.

FDP_ACF.1.1	The TSF shall enforce the [assignment: access control SFP] to objects based on the following: [assignment: list of subjects and objects controlled under the indicated SFP, and for each, the SFP-relevant security attributes, or named groups of SFP-relevant security attributes]. [Assignment: list of subjects and objects controlled under the indicated SFP, and for each, the SFP-relevant security attributes, or named groups of SFP-relevant security attributes] - Refer to “Table 6: Subject and corresponding security attribute (Disk_eject)”

	- Refer to "Table 7: Object and corresponding security attribute (Disk_eject)" [Assignment: access control SFP] Controlled Distribution SFP
FDP_ACF.1.2	The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [assignment: rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects]. [Assignment: rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects] - Only in the following case, allows checking the job information and disc position information. User identifier [Appli] associated with the process of the user who creates discs and user identifier [Appli] associated with the job information matches, and job ID associated with the job information and job ID associated with the disc position information matches. - Only in the following case, allows to change the job information, and change and delete disc position information. Job execution is completed
FDP_ACF.1.3	The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: [assignment: rules, based on security attributes that explicitly authorize access of subjects to objects]. [Assignment: rules, based on security attributes, that explicitly authorize access of subjects to objects] None
FDP_ACF.1.4	The TSF shall explicitly deny access of subjects to objects based on the [assignment: rules, based on security attributes that explicitly deny access of subjects to objects]. [Assignment: rules, based on security attributes, that explicitly deny access of subjects to objects] None

Dependencies: FDP_ACC.1 Subset access control

Dependencies: FMT_MSA.3 Static attribute initialization

Table 6: Subject and corresponding security attribute (Disk_eject)

Controlled subject	Corresponding SFP related security attribute
Process of the user who creates discs	User identifier [Appli]

Table 7: Object and corresponding security attribute (Disk_eject)

Controlled object	Corresponding SFP related security attribute
Job information	User identifier [Appli], JOB ID
Disc position information	JOB ID

FMT_MSA.3 Static attribute initialization

Hierarchical to: No other components.

FMT_MSA.3.1	The TSF shall enforce the [assignment: access control SFP, information flow control SFP] to provide [selection, choose one of: restrictive, permissive, [assignment: other property]] default values for security attributes that are used to enforce the SFP. [Selection, choose one of: restrictive, permissive, [assignment: other property]] [Assignment*:* other property] Unique identifier [Assignment: access control SFP, information flow control SFP] Controlled Distribution SFP
FMT_MSA.3.2	The TSF shall allow the [assignment: the authorized identified roles] to specify alternative initial values to override the default values when an object or information is created. [Assignment: the authorized identified roles] None.

Dependencies: FMT_MSA.1 Management of security attributes

Dependencies: FMT_SMR.1 Security roles

FDP_ACC.1[Cover_open] Subset access control

Hierarchical to: No other components.

FDP_ACC.1.1	The TSF shall enforce the [assignment: access control SFP] on [assignment: list of subjects, objects, and operations among subjects and objects covered by the SFP]. [Assignment: list of subjects, objects, and operations among subjects and objects covered by the SFP] Subject: - Administrator process Object: - Electronic lock Operations among subjects and objects covered by the SFP: - Deactivate the electronic lock [Assignment: access control SFP] Cover open control SFP

Dependencies: FDP_ACF.1 Security attribute based access control

FDP_ACF.1[Cover_open] Security attribute based access control

Hierarchical to: No other components.

FDP_ACF.1.1	The TSF shall enforce the [assignment: access control SFP] to objects based on the following: [assignment: list of subjects and objects controlled under the indicated SFP, and

	for each, the SFP-relevant security attributes, or named groups of SFP-relevant security attributes]. [Assignment: list of subjects and objects controlled under the indicated SFP, and for each, the SFP-relevant security attributes, or named groups of SFP-relevant security attributes] - Refer to “Table 8: Subject and corresponding security attribute (Cover_open) - Refer to “Table 9: Object and corresponding security attribute (Cover_open) [Assignment: access control SFP] Cover open control SFP
FDP_ACF.1.2	The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [assignment: rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects]. [Assignment: rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects] - Only in the following case, allows to deactivate the electronic lock. When confirmed that the administrator process has the administrator authority.
FDP_ACF.1.3	The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: [assignment: rules, based on security attributes that explicitly authorize access of subjects to objects]. [Assignment: rules, based on security attributes, that explicitly authorize access of subjects to objects] None
FDP_ACF.1.4	The TSF shall explicitly deny access of subjects to objects based on the [assignment: rules, based on security attributes that explicitly deny access of subjects to objects]. [Assignment: rules, based on security attributes, that explicitly deny access of subjects to objects] None

Dependencies: FDP_ACC.1 Subset access control

Dependencies: FMT_MSA.3 Static attribute initialization

Table 8: Subject and corresponding security attribute (Cover_open)

Controlled subject	Corresponding SFP related security attribute
Administrator process	Administrator authority

Table 9: Object and corresponding security attribute (Cover_open)

Controlled object	Corresponding SFP related security attribute
Electronic lock	None

FMT_MSA.1 Management of security attributes

Hierarchical to: No other components.

FMT_MSA.1.1	The TSF shall enforce the [assignment: access control SFP, information flow control SFP] to restrict the ability to [selection: change_default, query, modify, delete, [assignment: other operations]] the security attributes [assignment: list of security attributes] to [assignment: the authorized identified roles]. [Assignment: list of security attributes] Refer to “Security attributes” in “Table 10: List of operations for security attribute” [Selection: change_default, query, modify, delete, [assignment: other operations] Refer to “User operations” in “Table 10: List of operations for security attribute” [Assignment: the authorized identified roles] Refer to “Role” in “Table 10: List of operations for security attribute” [Assignment: access control SFP, information flow control SFP] Setting information management control SFP

Dependencies: [FDP_ACC.1 Subset access control or FDP_IFC.1 Subset information flow control]

Dependencies: FMT_SMF.1 Specification of Management Functions

Dependencies: FMT_SMR.1 Security roles

Table 10: List of operations for security attribute

Security attributes	User operations	Role
User identifier [Appli]	Inquiry	Administrator
JOB ID	None	None
Administrator authority	Query, change	Administrator

FMT_SMR.1 Security roles

Hierarchical to: No other components.

FMT_SMR.1.1	The TSF shall maintain the roles [assignment: the authorized identified roles]. [Assignment: the authorized identified roles] - Administrator - Publisher (person in charge of publishing discs) - Approver
FMT_SMR.1.2	The TSF shall be able to associate users with roles.

Dependencies: FIA_UID.1 Timing of identification

FMT_SMF.1 Specification of Management Functions

Hierarchical to: No other components.

FMT_SMF.1.1	The TSF shall be capable of performing the following security management functions: [assignment: list of security management functions to be provided by the TSF].

	[Assignment: list of security management functions to be provided by the TSF] Refer to “Table 11: Security management function list”.

Dependencies: No dependencies.

Table 11: Security management function list

Functional requirement	Management requirement	Security management function
FAU_ARP.1	a) The management of the actions (add, delete, change)	a) No management function since the action cannot be changed.
FAU_SAA.1	a) Maintaining the rules by (adding, changing, deleting) the rule in the rules.	a) No management function since the rules cannot be changed.
FAU_GET.1	None	---
FIA_UAU.2[Panel]	Management of the authentication data by an administrator; Management of the authentication data by the user associated with this data.	Functions for adding, changing, or deleting Password[Panel]
FIA_UID.2[Panel]	a) The management of the user identities.	a) Functions for inquiring, adding or deleting user identifier[Panel]
FIA_UAU.7[Panel]	None	---
FIA_AFL.1[Panel]	a) The management of the threshold value for unsuccessful authentication attempts b) The management of the action on authentication failure	a) No management function since the threshold value is fixed. b) No management function since the action cannot be changed.
FIA_SOS.1[Panel]	a) The management of the metric used to verify the secrets.	a) No management function since the metric cannot be changed.
FIA_UAU.2[Appli]	Management of the authentication data by an administrator; Management of the authentication data by the user associated with this data.	Functions for adding, changing, or deleting Password[Appli]
FIA_UID.2[Appli]	a) The management of the user identities.	a) Functions for inquiring, adding or deleting user identifier[Appli]
FIA_AFL.1[Appli]	a) The management of the threshold value for unsuccessful authentication attempts b) The management of the action on authentication failure	a) No management function since the threshold value is fixed. b) No management function since the action cannot be changed.
FIA_SOS.1[Appli]	a) The management of the metric used to verify the secrets.	a) No management function since the metric cannot be changed.

FDP_ETC.1	None	---
FDP_ACC.1[Disk_eject]	None	---
FDP_ACF.1[Disk_eject]	a) The management of the attribute used for decision based on explicitly denial or access	a) Functions for inquiring, adding or deleting user identifier[Appli]
FMT_MSA.3	a) Managing the group of roles that can specify initial values; b) Managing the permissive or restrictive setting of default values for a given access control SFP.	a) No management function since the group of roles that can specify initial values cannot be changed. b) No management function since the default values cannot be changed.
FDP_ACC.1[Cover_open]	None	---
FDP_ACF.1[Cover_open]	a) The management of the attribute used for decision based on explicitly denial or access	a) Function for inquiring or changing administrator privilege
FMT_MSA.1	a) Managing the group of roles that can interact with the security attribute	a) No management function since the group of roles that can interact with the security attribute cannot be changed.
FMT_SMR.1	a) Managing the group of users that are part of a role.	a) No management function since the group of users that are part of a role cannot be changed.
FMT_SMF.1	None	---
FIA_USB.1	a) Authorized administrator can define the default of subjects‘ security attributes. b) Authorized administrator can change the default of subjects‘ security attributes.	a) No management function since the default security attributes can not be defined. b) Functions for inquiring, or changing the security attributes.
FIA_ATD.1	a) If indicated to do so in the assignment, the authorized administrator can define additional security attributes to the users.	a) No management function since there is no need to add the security attributes.
FMT_MTD.1	a) Managing the group of roles that can interact with the TSF data.	a) No management function since the group of roles that can interact with the TSF data cannot be changed.
FMT_MOF.1	a) Managing the group of roles that can interact with the TSF function.	a) No management function since the group of roles that can interact with the TSF function cannot be changed.
FPT_RVM.1	None	---
FPT_SEP.1	None	---

FIA_USB.1 User-subject binding

Hierarchical to: No other components.

FIA_USB.1.1	The TSF shall associate the following user security attributes with subjects acting on the behalf of that user: [assignment: list of user security attributes]. [Assignment: list of user security attributes] - Administrator authority - User identifier [Appli]
FIA_USB.1.2	The TSF shall enforce the following rules on the initial association of user security attributes with subjects acting on the behalf of users: [assignment: rules for the initial association of attributes]. [Assignment: rules for the initial association of attributes] The TSF associates the user identifier [Appli] with the subjects that act on behalf of the user when the server control software authenticates the user upon a request from the control panel. In addition, when the user is the administrator, the TSF associates the administrator authority with the subject that acts on behalf of the user.
FIA_USB.1.3	The TSF shall enforce the following rules governing changes to the user security attributes associated with subjects acting on the behalf of users: [assignment: rules for changing attributes]. [Assignment: rules for changing attributes] None

Dependencies: FIA_ATD.1 User attribute definition

FIA_ATD.1 User attribute definition

Hierarchical to: No other components.

FIA_ATD.1.1	The TSF shall maintain the following list of security attributes belonging to individual users: [assignment: list of security attributes]. [Assignment: list of security attributes] - Administrator authority - User identifier [Appli]

Dependencies: No dependencies.

FMT_MTD.1 Management of TSF data

Hierarchical to: No other components.

FMT_MTD.1.1	The TSF shall restrict the ability to [selection: change_default, query, modify, delete, clear, [assignment: other operations]] the [assignment: list of TSF data] to [assignment: the authorized identified roles].

	[Assignment: list of TSF data] Refer to “TSF data” in “Table 12: List of operations for TSF data” [Selection: change_default, query, modify, delete, clear, [assignment: other operations]] Refer to “User operations” in “Table 12: List of operations for TSF data” [assignment: the authorized identified roles] Refer to “Role” in “Table 12: List of operations for TSF data”

Dependencies: FMT_SMF.1 Specification of Management Functions

Dependencies: FMT_SMR.1 Security roles

Table 12: List of operations for TSF data

TSF Data		User operations	Role
User information		Deletion The other operation: addition	Administrator
	User identifier [Appli] User identifier [Panel]	Query	
	Password [Appli] Password [Panel]	Change	
	Privilege	Query, change	
	Account lock status	Query, change	
Setting information	Security mode status	Query, change	
	Time setting information	Query, change	
	Network setting information	Query, change	
Job information	Job information	Query, change, deletion	
User information	The user’s password [Appli] The user’s password [Panel]	Change	Publisher
User information	The user’s password [Appli] The user’s password [Panel]	Change	Approver
Job information	Job information	Change	
Job information	Job information	Query, change The other operation: addition	Administrator Publisher Approver
Disc position information	Disc position information	Query, change The other operation: addition	

FMT_MOF.1 Management of security functions behavior

Hierarchical to: No other components.

FMT_MOF.1.1	The TSF shall restrict the ability to [selection: determine the behavior of, disable, enable,

	modify the behavior of] the functions [assignment: list of functions] to [assignment: the authorized identified roles]. [Assignment: list of functions] - Security mode [Selection: determine the behavior of, disable, enable, modify the behavior of] - Disable - Enable [Assignment: the authorized identified roles] Administrator

Dependencies: FMT_SMF.1 Specification of Management Functions

Dependencies: FMT_SMR.1 Security roles

FPT_RVM.1 Non-bypassability of the TSP

Hierarchical to: No other components.

FPT_RVM.1.1	The TSF shall ensure that TSP enforcement functions are invoked and succeed before each function within the TSC is allowed to proceed.

Dependencies: No dependencies.

FPT_SEP.1 TSF domain separation

Hierarchical to: No other components.

FPT_SEP.1.1	The TSF shall maintain a security domain for its own execution that protects it from interference and tampering by untrusted subjects.
FPT_SEP.1.2	The TSF shall enforce separation between the security domains of subjects in the TSC.

Dependencies: No dependencies.

5.1.2 TOE Security Assurance Requirements

The table below lists the TOE security assurance requirements.

Table 13: TOE security assurance requirements

Class	Component name (including family)
Assurance Configuration Management	ACM_CAP.3 Management of allowing
	ACM_SCP.1 CM scope of TOE
Assurance Delivery and Operation	ADO_DEL.1 Delivery procedures
	ADO_IGS.1 Installation, generation, and start-up procedures
Assurance Development	ADV_FSP.1 Informal functional specification
	ADV_HLD.2 Development of upper level security enforcement
	ADV_RCR.1 Informal correspondence demonstration
Assurance Guidance Document	AGD_ADM.1 Administrator guidance

	AGD_USR.1 User guidance
Assurance Life Cycle support	ALC_DVS.1 Identification of security method
Assurance Test	ATE_COV.2 Analysis of the coverage
	ATE_DPT.1 Test: Design of upper level
	ATE_FUN.1 Functional testing
	ATE_IND.2 Independent testing - sample
Assurance Vulnerability Assessment	AVA_MSU.1 Inspection of guidance
	AVA_SOF.1 Strength of TOE security function evaluation
	AVA_VLA.1 Developer vulnerability analysis

5.1.3 Minimum Strength of Function

The minimum strength of function for this TOE is SOF-basic. The table below lists the target TOE security functional requirements and the minimum strength of function.

Table 14 TOE security functional requirements and function strength

TOE security functions	Claimed strength
FIA_UAU.2[Panel]	SOF-basic
FIA_AFL.1[Panel]	SOF-basic
FIA_SOS.1[Panel]	SOF-basic
FIA_UAU.2[Appli]	SOF-basic
FIA_AFL.1[Appli]	SOF-basic
FIA_SOS.1[Appli]	SOF-basic

5.2 IT Security Requirements for the IT Environment

The security requirements for the IT environment are as follows.

FIA_UAU.7[Appli] Protected authentication feedback

Hierarchical to: No other components.

FIA_UAU.7.1	The <u>TSF</u> shall provide only [assignment: list of feedback] to the user while the authentication is in progress. [Assignment: list of feedback] Displays the same number of dummy characters, such as asterisks, as the entered characters [Details] (details of the above underlined word) TSF: Browser, Total Disc Maker and Total Disc Monitor

Dependencies: FIA_UAU.1 Timing of authentication

6 TOE Summary Specification

This chapter provides summarized specifications of the TOE security functions and security assurance measures.

6.1 TOE Security Functions

This section describes about TOE security functions, security mechanism, and the claimed strength of function.

6.1.1 TOE Security Functions

The table below lists the TOE security functions.

Table 15: Security Functions and Security Requirements

	SF.Controlled Distribution function	SF. Electronic Lock Open function	SF.Identify Authentication [Panel] function	SF.Identify Authentication [Web_app] function	SF.Identify Authentication [Cli_app] function	SF. Warning function	SF. Setting Data Control function
FAU_ARP.1						√	
FAU_SAA.1						√	
FAU_GET.1						√	
FIA_UAU.2[Panel]			√				
FIA_UID.2[Panel]			√				
FIA_UAU.7[Panel]			√				
FIA_AFL.1[Panel]			√				
FIA_SOS.1[Panel]							√
FIA_UAU.2[Appli]				√	√		
FIA_UID.2[Appli]				√	√		
FIA_AFL.1[Appli]				√	√		
FIA_SOS.1[Appli]							√
FDP_ETC.1	√						
FDP_ACC.1[Disk_eject]	√						
FDP_ACF.1[Disk_eject]	√						
FMT_MSA.3	√						
FDP_ACC.1[Cover_open]		√					

FDP_ACF.1[Cover_open]		√					
FMT_MSA.1							√
FMT_SMR.1							√
FMT_SMF.1							√
FIA_USB.1							√
FIA_ATD.1							√
FMT_MTD.1	√						√
FMT_MOF.1							√
FPT_RVM.1	√	√	√	√	√		√
FPT_SEP.1	√	√	√	√	√	√	√

SF.Controlled Distribution function

This function allows only the user who created discs to take out the published discs.

- The user presses the EJECT button on the PP-100N control panel.
- The TOE activates the SF.Identify Authentication [Panel] function to identify the user.
- The TOE terminates the disc ejection process if the SF.Identify Authentication [Panel] function finds the user has not been registered.
- If the user is found as a registered user by the function, the TOE checks the job information, which is an object of the Controlled Distribution SFP. TOE has associated a unique user identifier [Appli] and the job ID with the job information. The association is not changed. {FDP_ACC.1[Disk_eject], FDP_ACF.1[Disk_eject], FMT_MTD.1, FMT_MSA.3}
- When the TOE finds that discs published by the user exist in PP-100N by the job information check, the TOE then checks the disc position information. With the information, which is an object of the Controlled Distribution SFP, a unique job ID has been associated by the TOE, and the association is not changed. {FDP_ACC.1[Disk_eject], FDP_ACF.1[Disk_eject], FMT_MTD.1, FMT_MSA.3}
- When the TOE determines that no published discs exit in PP-100N for the user, the TOE terminates the disc ejection process.
- On the basis of the disc position information, the TOE moves the autoloader to transfer the discs to Stacker 4. {FDP_ETC.1}
- When transferring discs to Stacker 4 is finished, the TOE changes or deletes the disc position information. {FMT_MTD.1}
- The TOE activates the SF.Controlled Distribution function when the user ejects the discs to ensure the success of the access restriction. {FPT_RVM.1}
- The TSF related to the SF.Controlled Distribution function protects itself from being interfered or tampered. {FPT_SEP.1}

SF. Electronic Lock Open function

This function allows the administrator to control the electronic lock when he or she opens the disc cover.

- The administrator selects the menu for deactivating the electronic lock on the control panel of PP-100N.
- The TOE activates the SF.Identify Authentication [Panel] function to identify the user.

- The TOE terminates the operation if the SF.Identify Authentication [Panel] function finds the user is not the administrator.
- If the user is identified as the administrator by the function, the TOE deactivates the electronic lock. {FDP_ACC.1[Cover_open], FDP_ACF.1[Cover_open]}
- The TOE activates the electronic lock if the disc cover is not opened within five seconds after the lock is deactivated.
- The TOE activates the SF. Electronic Lock Open function during the disc cover open process by the administrator to ensure the success of the access restriction. {FPT_RVM.1}
- The TSF related to the SF. Electronic Lock Open function protects itself from being interfered or tampered. {FPT_SEP.1}

SF.Identify Authentication [Panel] function

This function identifies an authorized user who accesses to the TOE using the control panel of PP-100N.

- The SF.Identify Authentication [Panel] function is activated when a user is operating the control panel and the user identity authentication is required.
- The TOE does not accept any operations until the identity authentication is executed. {FIA_UAU.2[Panel], FIA_UID.2[Panel]}
- The user is required to enter his/her user identifier [Panel] and password [Panel].
- The TOE makes the LCD to display the same number of "*" (asterisks) as the entered characters. {FIA_UAU.7[Panel]}
- The TOE compares the entered user identifier [Panel] and password [Panel] to registered user information, and determines that the user is authenticated when a match is detected. If no match is found, the TOE prompts the user to reenter the identification [Panel] and password [Panel].
- When the TOE failed the user identify authentication three times in a row during a given time, the TOE locks the user account to prevent the user from logging in using the control panel. The TOE automatically unlocks the user account after six hours for an administrator, and after one hour for the other users. {FIA_AFL.1[Panel]}
- The TOE ensures the success of user identity authentication with the SF.Identify Authentication [Panel] function before any action using the TSC function is allowed. {FPT_RVM.1}
- The TSF related to the SF.Identify Authentication [Panel] function protects itself from being interfered or tampered. {FPT_SEP.1}

SF.Identify Authentication [Web_app] function

This function identifies an authorized user who accesses to the TOE using the PP-100N Web application.

- When the PP-100N Web application is started, a user identify authentication screen is displayed.
- The TOE does not accept any operations until the identity authentication is executed. {FIA_UAU.2[Appli], FIA_UID.2[Appli]}
- The user is required to enter his/her user identifier [Appli] and password [Appli].
- The TOE compares the entered user identifier [Appli] and password [Appli] to registered user information, and determines that the user is authenticated when a match is detected. If no match is found, the TOE

prompts the user to reenter the identification [Appli] and password [Appli].

- When the TOE failed the user identify authentication three times in a row during a given time, the TOE locks the user account to prevent the user from logging in using the PP-100N Web application. The TOE automatically unlocks the user account after six hours for an administrator, and after one hour for the other users. {FIA_AFL.1[Appli]}
- The TOE ensures the success of user identify authentication with the SF.Identify Authentication [Web_app] function before any action using the TSC function is allowed. {FPT_RVM.1}
- The TSF related to the SF.Identify Authentication [Web_app] function protects itself from being interfered or tampered. {FPT_SEP.1}

SF.Identify Authentication [Cli_app] function

This function identifies an authorized user who accesses to the TOE using the Total Disc Maker or Total Disc Monitor.

- When the TOE detects an access from Total Disc Maker or Total Disc Monitor, a user identify authentication screen is displayed.
- The TOE does not accept any operations until the identify authentication is executed. {FIA_UAU.2[Appli], FIA_UID.2[Appli]}
- The user is required to enter his/her user identifier [Appli] and password [Appli].
- The TOE compares the entered user identifier [Appli] and password [Appli] to registered user information, and determines that the user is authenticated when a match is detected. If no match is found, the TOE prompts the user to reenter the identification [Appli] and password [Appli].
- When the TOE failed the user identify authentication three times in a row during a given time, the TOE locks the user account to prevent the user from logging in using Total Disc Maker or Total Disc Monitor. The TOE automatically unlocks the user account after six hours for an administrator, and after one hour for the other users. {FIA_AFL.1[Appli]}
- The TOE ensures the success of user identity authentication with the SF.Identify Authentication [Cli_app] function before any action using the TSC function is allowed. {FPT_RVM.1}
- The TSF related to the SF.Identify Authentication [Cli_app] function protects itself from being interfered or tampered. {FPT_SEP.1}

SF. Warning function

This function warns the administrator of security problems.

- The TOE warns the administrator using the following methods whenever it detects any of (1) to (5) conditions and judges that there is possibility of security problem.
  - Sounds a buzzer
  - Turns on the ERROR LED
  - Displays a solution on the LCD

(1) When turning off the power

During the power-off process, alerts the administrator that published discs exist in PP-100N.

- The TOE checks job information whether published discs exist or not, and whether processing jobs exist or not. {FAU_GET.1}

- The TOE continues the power-off process if no published discs and processing jobs is detected.
- When either of published discs or processing job existence is found, the TOE judges that there is a possibility of security problem. {FAU_SAA.1}

(2) When the disc cover is open

Alerts the administrator that the disc cover is kept open.

- The TOE detects that the disc cover is opened with the disc cover detector. {AU_GET.1}
- When the TOE does not detect that the cover is closed within 60 seconds, it judges that there is a possibility of security problem. {FAU_SAA.1}

(3) When the disc cover is closed

Alerts the administrator that the disc cover is not physically locked or the security lock switch is off.

- After the disc cover is closed by someone, the TOE detects that the cover is not physically locked or the security lock switch is off with the disc cover detector and lock position detector. {FAU_GET.1}
- If the above status is continued for more than 10 seconds, the TOE judges that there is a possibility of security problem. {FAU_SAA.1}

(4) When feeding discs

Alerts the administrator that the autoloader drops a disc during its disc feeding operation.

- The TOE detects that the autoloader drops a disc with the disc detector. {FAU_GET.1}
- The TOE judges that there is a possibility of security problem. {FAU_SAA.1}

(5) When removing Stacker 2

Alerts the administrator that discs exist in Stacker 2 when the stacker is removed with PP-100N powered on.

- With the disc cover detector and Stacker 2 detector, the TOE detects that Stacker 2 is removed and attached while the disc cover is open. {FAU_GET.1}
- After the disc cover is closed, with the disc cover detector and disc detector, the TOE detects that discs exist in Stacker 2. {FAU_GET.1}
- The TOE judges that there is a possibility of security problem when discs exist in Stacker 2 after the stacker is removed and reattached. {FAU_SAA.1}

Common to (1) to (5)

- The TSF related to the SF. Warning function protects itself from being interfered or tampered. {FPT_SEP.1}

SF. Setting Data Control function

This function restricts the following accesses to authorized users; “access from a client PC to the setting control data, job information, or disc position information” and “access to the setting control data from the PP-100N control panel”.

(1) Access restriction

- The TOE defines and maintains the following security attributes. {FIA_ATD.1}
  - User identifier [Appli]
  - Administrator authority
- The TOE associates the user identifier [Appli] with the subject that acts for the user authorized by the SF.Identify Authentication [Panel] function. In addition, when the user is the administrator, the TOE

associates the administrator authority with the subject that acts for the user.

- The TOE classifies the user authorized by SF.Identify Authentication [Panel] function, SF.Identify Authentication [Web_app] function, or SF.Identify Authentication [Cli_app] function, into any one of the following roles, and keeps the role unchanged.
    - Administrator
    - Approver
    - Publisher
- The TOE allows only the administrator to make settings of security functions. {FMT_MOF.1}
- As listed in Table 16, the TOE restricts user operations in accordance with the authorized user role. {FMT_MSA.1, FMT_MTD.1, FMT_SMF.1}

Table 16: Available User Operations by Authorized User Role

Role	TSF data		User operations
Administrator	User information		Deletion The other operation: addition
		User identifier [Appli] User identifier [Panel]	Query
		Password [Appli] Password [Panel]	Change
		Privilege	Query, change
		Account lock status	Query, change
	Setting information	Security mode status	Query, change
		Time setting information	Query, change
		Network setting information	Query, change
	Job information	Job information	Query, change, deletion
Publisher	User information	The user’s password [Appli] The user’s password [Panel]	Change
Approver	User information	The user’s password [Appli] The user’s password [Panel]	Change
	Job information	Job information	Change
The other users	Job information	Job information	Query, change The other operation: addition
	Disc position information	Disc position information	The other operation: addition

(2) Password change function

- When a password change is requested, the TOE displays a new password string replacing the entered characters with the other characters. The character replacement is performed based on the OS, which is the IT environment.
- The TOE checks if the password meets the following requirements. {FIA_SOS.1[Panel], FIA_SOS.1[Appli]}
    - Password [Panel]: five or more numeric characters

- Password [Appli]: five or more alphanumeric characters or special characters (“.”, “–“, “_”)

(3) Other functions

- The TOE ensures the success of access restriction to the setting control information, job information, and disc position information by activating the SF. Setting Data Control function. {FPT_RVM.1}
- The TSF related to the SF. Setting Data Control function protects itself from being interfered or tampered. {FPT_SEP.1}

6.1.2 TOE Security Function Strength

Table 17 lists the TOE security functions that are based on unencrypted and probabilistic or permutational mechanism and their claimed strength.

Table 17: TOE Security Functions and Claimed Strength

TOE security functions	Claimed strength
SF.Identify Authentication [Panel] function	SOF-basic
SF.Identify Authentication [Web_app] function	SOF-basic
SF.Identify Authentication [Cli_app] function	SOF-basic
SF.Setting Data Control function	SOF-basic

6.2 Assurance Measures

Table 18 lists the document provided to support security assurance.

Table 18: List of Assurance Measures Document

Classification	Component	Document name and TOE
ACM (Assurance Configuration Management)	ACM_CAP.3	- KP-01 PP-100N Configuration Management Plan (overall product) - KP-02 PP-100N Configuration Management Plan (mechanism) - KP-03 PP-100N Configuration Management Plan (autoloader board) - KP-04 PP-100N Configuration Management Plan (server system software) - KP-05 PP-100N Configuration Management Plan (autoloader firmware) - KL-01 PP-100N Configuration List (overall product) - KL-02 PP-100N Configuration List (mechanism) - KL-03 PP-100N Configuration List (autoloader board) - KL-04 PP-100N Configuration List (server system software) - KL-05 PP-100N Configuration List (autoloader firmware)
	ACM_SCP.1	- KL-01 PP-100N Configuration List (overall product) - KL-02 PP-100N Configuration List (mechanism) - KL-03 PP-100N Configuration List (autoloader board) - KL-04 PP-100N Configuration List (server system software) - KL-05 PP-100N Configuration List (autoloader firmware)
ADO (Assurance Delivery and Operation)	ADO_DEL.1	- PP-100N Delivery Procedure Manual - PP-100N Web Delivery Procedure Manual
	ADO_IGS.1	- PP-100N Security Administrator’s Guide - Install Manual for PP-100N - Sheet, Security, PP100N

ADV (Assurance Development)	ADV_FSP.1	- Seiko Epson PP-100N Security Control Unit Functional Specifications - Seiko Epson PP-100N Security Control Unit TOE Functions Diagram
	ADV_HLD.2	- Seiko Epson PP-100N Security Control Unit High-Level Design Specifications - Seiko Epson PP-100N Security Control Unit TOE Subsystem Diagram
	ADV_RCR.1	- Seiko Epson PP-100N Security Control Unit Representation Correspondence Analysis Report
AGD (Assurance Guidance Document)	AGD_ADM.1	- PP-100N Security Administrator's Guide - Sheet, Security, PP100N
	AGD_USR.1	- PP-100N Security User's Guide
ALC (Assurance Life Cycle support)	ALC_DVS.1	- PP-100N Security Control Unit Security Standard of Development
ATE (Assurance Test)	ATE_COV.2	- PP-100N Security Control Unit Functional Test Report - PP-100N Security Control Unit High-Level Design Test Report
	ATE_DPT.1	
	ATE_FUN.1	
	ATE_IND.2	
AVA (Assurance Vulnerability Assessment)	AVA_MSU.1	- PP-100N Security Control Unit Analysis Report on improper use
	AVA_SOF.1	- PP-100N Security Control Unit Functional Strength Analysis Report
	AVA_VLA.1	- PP-100N Security Control Unit Vulnerability Analysis Report

7 PP Claims

This ST does not claim conformance to any PP.

8 Rationale

This chapter describes the rationales for security objectives, security requirements, TOE summary specifications, and PP claim.

8.1 Security Objectives Rationale

This section describes why the security objectives are needed and the reason why the objectives are sufficient.

8.1.1 Need of Security Objectives

Table 19 lists the security objectives showing under which TOE security environment they are used.

Table 19: Security Objectives vs TOE Security Environment

	A.Approver	A.Administrator	A.Password	A.Operation status management	A.Security mode	A.Network	T.Taking out of discs	T.Disc cover unlocked	T.Dropping of discs	T.Misplacement of discs	P.Published discs
O.Identify Authentication							√				
O.Controlled Distribution							√				
O.Cover open restriction							√				
O.Registration management							√				
O.Warning								√	√	√	√
OE.Reliability of approver	√										
OE.Reliability of administrator		√									
OE.Password management			√								
OE.Handling by administrator								√	√	√	√
OE.Monitoring by administrator				√							
OE.Security mode setting					√						
OE.Network						√					
OI.Password security							√				

As shown in Table 19, all of the security objectives correspond to at least one TOE security environment. Thus, the need for security objectives is satisfied.

8.1.2 Sufficiency of Security Objectives

A. Approver

The “OE. Reliability of approver” is achieved by a responsible of the organization. He/She appoints a reliable person as the approver. Thus, the “A. Approver” can be realized.

A. Administrator

The “OE. Reliability of administrator” is achieved by a responsible of the organization. He/She appoints reliable persons as the administrators and educates them. Thus, the “A. Administrator” can be realized.

A. Password

The “OE. Password management” instructs the users to set their own password properly, how often the password should be changed according to the TOE Guidance document, and not to reveal the password to anyone. Thus the “A. Password” can be realized.

A. Operation status management

The “OE. Monitoring by administrator” means that the administrator monitors PP-100N operation status to prevent the followings from occurring.

- Destroying PP-100N
- Unlocking of the disc cover by anyone except the administrator

Thus the “A. Operation status management” can be realized.

A. Security mode

The “OE. Security mode setting” is made by the administrator as follows; he/she connects the authentication keypad to PP-100N included in the security pack, and makes security mode setup for the PP-100N. Thus the “A. Security mode” can be realized.

A. Network

The “OE. Network” requires the administrator to take measures against intrusion from external network, and protect the internal network from being bugged. Thus the “A. Network” can be realized.

T. Taking out of discs

The “O. Registration management” allows the administrator to manage the user information (user identifier, password, and etc.) that is required for user authentication. Because each user can change his/her own password [Panel] and password [Appli], the user authentication can be made by each user. The entered password can remain completely secret; password [Panel] is protected by the “O. Identify Authentication”, and password [Appli] is protected by the “OI. Password security”. When the user takes out discs published by him/herself, the “O. Identify Authentication” is used to identify the published user, and the “O. Controlled Distribution” allows only the published user to take out the discs. When the administrator opens the disc cover, the “O. Identify Authentication” is used to identify the administrator, and the “O. Cover open restriction” allows only the administrator to open the cover. These make it impossible that anyone except the published user and the administrator take out published discs, thus prevents unintended “T. Taking out of disc”.

T. Disc cover unlocked

The “O. Warning” alerts a disc cover unlocked status to the administrator. In such case, the “OE. Handling by administrator” is an administrator’s prompt action to lock the disc cover. Thus, the “T. Disc cover unlocked” risk can be reduced.

T. Dropping of discs

The “O. Warning” alerts the administrator when the autoloader drops discs. In such case, the “OE. Handling by administrator” is an administrator’s prompt action to remove the dropped discs. Any discs dropped by the autoloader are not subjected to anyone except the administrator and the published user, thus the “T. Dropping of discs” risk can be reduced.

T. Misplacement of discs

Using the “O. Warning”, the administrator or service person can alert a disc misplacement error to the administrator. According to the information of disc existence in Stacker 2 that has been removed and reattached with PP-100N powered on, the administrator or service person can judge that the error might have occurred. In such case, the “OE. Handling by administrator” is an administrator’s prompt action to remove the discs from Stacker 2. This prevents discs being incorrectly ejected due to the misplacement, and thus the “T. Misplacement of discs” risk can be reduced.

P. Published discs

The “O. Warning” alerts the administrator when published discs are detected in PP-100N during the power-off process. In such case, the “OE. Handling by administrator” is an administrator’s prompt action to remove the published discs from PP-100N. Thus the “P. Published discs” can be protected.

8.2 Security Requirements Rationale

This section describes why the security functional requirements are needed, the reason why the requirements are sufficient, the adequacy of the requirements dependencies, how the requirements are interrelated, the adequacy of the minimum functional strength, the adequacy of the evaluation assurance level, and why the security assurance requirements are needed.

8.2.1 Need of Security Functional Requirements

Table 20 indicates which TOE security functional requirement corresponds to which TOE security objectives.

Table 20: TOE Security Functional Requirements vs TOE Security Objectives

	O.Identify authentication	O.Controlled distribution	O.Cover open control	O.Registration management	O.Warning
FAU_ARP.1					√
FAU_SAA.1					√
FAU_GET.1					√
FIA_UAU.2[Panel]	√				
FIA_UID.2[Panel]	√				
FIA_UAU.7[Panel]	√				
FIA_AFL.1[Panel]	√				
FIA_SOS.1[Panel]				√	
FIA_UAU.2[Appli]	√				
FIA_UID.2[Appli]	√				
FIA_AFL.1[Appli]	√				
FIA_SOS.1[Appli]				√	
FDP_ETC.1		√			
FDP_ACC.1[Disk_eject]		√			
FDP_ACF.1[Disk_eject]		√			
FMT_MSA.3		√			
FDP_ACC.1[Cover_open]			√		
FDP_ACF.1[Cover_open]			√		
FMT_MSA.1				√	
FMT_SMR.1				√	
FMT_SMF.1				√	
FIA_USB.1				√	
FIA_ATD.1				√	
FMT_MTD.1		√		√	
FMT_MOF.1				√	
FPT_RVM.1	√	√	√	√	
FPT_SEP.1	√	√	√	√	√

As shown in Table 20, all of the security functional requirements correspond to at least one TOE security objectives. Thus, the need for TOE security functional requirements is satisfied. Table 21 shows the correspondences between security functional requirements and security objectives for the IT environment.

Table 21: Security functional requirements VS Security objectives for the IT environment

	OI.Password security
FIA_UAU.7[Appli]	√

As shown in Table 21, all of the IT environment security functional requirements correspond to at least one IT environment security objectives. Thus, the need for IT environment security functional requirements is satisfied.

8.2.2 Sufficiency of Security Functional Requirements

O.Identify Authentication

The "O.Identify Authentication" can be realized by FIA_UAU.2[Panel], FIA_UID.2[Panel], FIA_UAU.7[Panel], FIA_AFL.1[Panel], FIA_UAU.2[Appli], FIA_UID.2[Appli], FIA_AFL.1[Appli], FPT_RVM.1, and FPT_SEP.1.

<Login from the control panel>

- The TSF identifies and authenticates the user using FIA_UID.2[Panel] and FIA_UAU.2[Panel]. Until the authentication is finished, any other TOE operations are not accepted.
- Using FIA_UAU.7[Panel], the TSF makes the display to show the same number of "*" (asterisks) as the entered password characters to keep the password completely secret.
- Using FIA_AFL.1[Panel], when the TSF failed the user identify authentication three times in a row during a given time, the TSF locks the user account to prevent the user from logging in using the control panel. The TSF automatically unlocks the user account after six hours for an administrator, and after one hour for the other users.

<Login from the PP-100N Web application>

- The TSF identifies and authenticates the user using FIA_UID.2[Appli] and FIA_UAU.2[Appli]. Until the authentication is finished, any other TOE operations are not accepted.
- Using FIA_AFL.1[Appli], when the TSF failed the user identify authentication three times in a row during a given time, the TSF locks the user account to prevent the user from logging in from the PP-100N Web application. The TSF automatically unlocks the user account after six hours for an administrator, and after one hour for the other users.

<Login from Total Disc Maker or Total Disc Monitor >

- The TSF identifies and authenticates the user using FIA_UID.2[Appli] and FIA_UAU.2[Appli]. Until the authentication is finished, any other TOE operations are not accepted.
- Using FIA_AFL.1[Appli], when the TSF failed the user identify authentication three times in a row during a given time, the TSF locks the user account to prevent the user from logging in from Total Disc Maker or Total Disc Monitor. The TSF automatically unlocks the user account after six hours for an administrator, and after one hour for the other users.

<Common to all the login operations >

- The TSF is called by FPT_RVM.1 without fail before any access control is activated.
- FPT_SEP.1 lets the TSF separate from the subject domains in order to protect the functional requirements from illegal access.

O. Controlled distribution

The “O. Controlled distribution” can be realized by FDP_ETC.1, FDP_ACC.1[Disk_eject], FDP_ACF.1[Disk_eject], FMT_MSA.3, FMT_MTD.1, FPT_RVM.1, FPT_SEP.1.

- The TSF ejects published discs using FDP_ETC.1.
- FDP_ACC.1[Disk_eject] lets the TSF to carry out access control for ejecting the discs only for the user who created them.
- FDP_ACF.1[Disk_eject] lets the TSF carry out access control according to the user identifier [Appli].
- Using FMT_MSA.3, the TSF sets a default unique identifier (user identifier [Appli]).
- FMT_MTD.1 lets the TSF control the TSF data, disc position information, so that a change or deletion of the information is made only when the user who published the discs operates to do so.
- The TSF is called by FPT_RVM.1 without fail every time the controlled distribution is performed.
- FPT_SEP.1 lets the TSF separate from the subject domains in order to protect the functional requirements from illegal access.

O. Cover open restriction

The “O. Cover open restriction” can be realized by FDP_ACC.1[Cover_open], FDP_ACF.1[Cover_open], FPT_RVM.1, FPT_SEP.1.

- FDP_ACC.1[Cover_open] lets the TSF carry out access control for opening the disc cover.
- FDP_ACF.1[Cover_open] lets the TSF restrict the access for opening the disc cover to the administrator.
- The TSF is called by FPT_RVM.1 without fail every time the cover open restriction is performed.
- FPT_SEP.1 lets the TSF separate from the subject domains in order to protect the functional requirements from illegal access.

O. Registration

The “O. Registration” can be realized by FIA_SOS.1[Panel], FIA_SOS.1[Appli], FMT_MSA.1, FMT_SMR.1, FMT_SMF.1, FIA_USB.1, FIA_ATD.1, FMT_MTD.1, FMT_MOF.1, FPT_RVM.1, FPT_SEP.1.

- FIA_SOS.1[Panel] lets the TSF verify a set password [Panel] if it satisfies an acceptable quality level.
- FIA_SOS.1[Appli] lets the TSF verify a set password [Appli] if it satisfies an acceptable quality level.
- FMT_MSA.1 lets the TSF manage the security attributes of the users.
- FMT_SMR.1 lets the TSF define and maintain each user role.
- FMT_SMF.1 lets the TSF specify a management function for a management requirement of each functional requirement.
- FIA_USB.1 lets the TSF associate the user with a subject that operates for the user.
- FIA_ATD.1 lets the TSF define and maintain each user’s security attribute.
- FMT_MTD.1 lets the TSF manage the TSF data so that each user operates the data within the limit

predetermined according to his/her role.

- FMT_MOF.1 lets the TSF allow only the administrator to set up the security functions.
- The TSF is called by FPT_RVM.1 without fail every time the registration is performed.
- FPT_SEP.1 lets the TSF separate from the subject domains in order to protect the functional requirements from illegal access.

O. Warning

In the following cases, there is a high possibility that a security problem is arising.

- Published discs are detected inside the PP-100N during a power-off process.
- The disc cover is left unlocked.
- The autoloader dropped discs.
- During the PP-100N is powered, discs are detected in Stacker 2 after the stacker is removed and reattached.

The “O. Warning” can be realized by FAU_GET.1, FAU_SAA.1, FAU_ARP.1, FPT_SEP.1.

- FAU_GET.1 lets the TSF acquire event logs to check if any of the above events that indicate a high possibility of security problem.
- FAU_SAA.1 lets the TSF analyze the event logs and judge if a warning is necessary or not.
- If the TSF judged that a warning is needed, FAU_APP.1 lets the TSF warn the administrator.
- FPT_SEP.1 lets the TSF separate from the subject domains in order to protect the functional requirements from illegal access.

OI. Password security

The “OI. Password security” can be realized by FIA_UAU.7[Appli].

<Login from PP-100N Web application>

- FIA_UAU.7[Appli] lets the browser display the same number of dummy characters, such as asterisks, as the entered characters to keep the password secret.

<Login from Total Disc Maker or Total Disc Monitor>

- FIA_UAU.7[Appli] lets the Total Disc Maker or Total Disc Monitor display the same number of dummy characters, such as asterisks, as the entered characters to keep the password secret.

8.2.3 Adequacy of Security Functional Requirements Dependencies

The table below lists the security functional requirements and their dependencies. This clarifies how the security functional requirements dependencies are satisfied. For the requirements that have no dependency, the reasons are described below the table.

Table 22: Security Functional Requirements Dependencies

No	TOE security functional requirements	Subordinate requirements	Dependencies	Reference No.	Remarks
1	FAU_ARP.1	---	FAU_SAA.1	2	
2	FAU_SAA.1	---	FAU_GEN.1	No need	See *1 note below

3	FAU_GET.1	---	---	---	
4	FIA_UAU.2[Panel]	FIA_UAU.1	FIA_UID.2[Panel]	5	The dependency is satisfied because FIA_UID.2 exists at a level upper than FIA_UID.1.
5	FIA_UID.2[Panel]	FIA_UID.1	---	---	
6	FIA_UAU.7[Panel]	---	FIA_UAU.2[Panel]	4	The dependency is satisfied because FIA_UAU.2 exists at a level upper than FIA_UAU.1.
7	FIA_AFL.1[Panel]	---	FIA_UAU.2[Panel]	4	The dependency is satisfied because FIA_UAU.2 exists at a level upper than FIA_UAU.1.
8	FIA_SOS.1[Panel]	---	---	---	
9	FIA_UAU.2[Appli]	FIA_UAU.1	FIA_UID.2[Appli]	10	The dependency is satisfied because FIA_UID.2 exists at a level upper than FIA_UID.1.
10	FIA_UID.2[Appli]	FIA_UID.1	---	---	
11	FIA_AFL.1[Appli]	---	FIA_UAU.2[Appli]	9	The dependency is satisfied because FIA_UAU.2 exists at a level upper than FIA_UAU.1.
12	FIA_SOS.1[Appli]	---	---	---	
13	FDP_ETC.1	---	FDP_ACC.1[Disk_eject]	14	
14	FDP_ACC.1[Disk_eject]	---	FDP_ACF.1[Disk_eject]	15	
15	FDP_ACF.1[Disk_eject]	---	FDP_ACC.1[Disk_eject]	14	
			FMT_MSA.3	16	
16	FMT_MSA.3	---	FMT_MSA.1	19	
			FMT_SMR.1	20	
17	FDP_ACC.1[Cover_open]	---	FDP_ACF.1[Cover_open]	18	
18	FDP_ACF.1[Cover_open]	---	FDP_ACC.1[Cover_open]	17	
			FMT_MSA.3	No need	See *2 note below

19	FMT_MSA.1	---	FDP_ACC.1[Disk_eject] FDP_ACC.1[Cover_open]	14 17	
			FMT_SMF.1	21	
			FMT_SMR.1	20	
20	FMT_SMR.1	---	FIA_UID.2[Panel] FIA_UID.2[Appli]	5 10	The dependency is satisfied because FIA_UID.2 exists at a level upper than FIA_UID.1.
21	FMT_SMF.1	---	---	---	
22	FIA_USB.1	---	FIA_ATD.1	23	
23	FIA_ATD.1	---	---	---	
24	FMT_MTD.1	---	FMT_SMF.1	21	
			FMT_SMR.1	20	
25	FMT_MOF.1	---	FMT_SMF.1	21	
			FMT_SMR.1	20	
26	FPT_RVM.1	---	---	---	
27	FPT_SEP.1	---	---	---	
28	FIA_UAU.7[Appli]	---	FIA_UAU.2[Appli]	4	The dependency is satisfied because FIA_UAU.2 exists at a level upper than FIA_UAU.1.

*1: Reason why FAU_GEN.1 dependency is not needed;
This TOE does not employ FAU_GEN.1. When this TOE judges that a security problem may be arising, it immediately warns the administrator about the problem, and the administrator is supposed to remove the causes. Therefore, monitor logs such as date and time information acquirable by FAU_GEN.1 are not needed. Instead of FAU_GEN.1, this TOE employs FAU_GET.1 in order to acquire some event logs needed for analyzing the possibility of security problems.

*2: Reason why FMT_MSA.3 dependency is not needed;
This TOE does not employ FMT_MSA.3. Because this TOE carry out controls according to the security attributes of subjects, those of objects are not needed. Therefore, there is no need to define the default of the object's security attributes.

In this way, the dependencies of the security functional requirements are adequate.

8.2.4 Interrelationships among Security Functional Requirements

The table below lists the interrelationships among security functional requirements. The interrelationships are consisted of deactivation prevention, bypass prevention and tampering prevention.

Table 23: Interrelationships among security functional requirements

Functional requirement	Functional requirements that offer prevention functions		
	Deactivation prevention	Bypass prevention	Tampering prevention
FAU_ARP.1	None	FPT_RVM.1	FPT_SEP.1
FAU_SAA.1	None	FPT_RVM.1	FPT_SEP.1
FAU_GET.1	None	FPT_RVM.1	FPT_SEP.1
FIA_UAU.2[Panel]	FMT_MOF.1	FPT_RVM.1	FPT_SEP.1
FIA_UID.2[Panel]	FMT_MOF.1	FPT_RVM.1	FPT_SEP.1
FIA_UAU.7[Panel]	None	FPT_RVM.1	FPT_SEP.1
FIA_AFL.1[Panel]	FMT_MOF.1	FPT_RVM.1	FPT_SEP.1
FIA_SOS.1[Panel]	None	FPT_RVM.1	FPT_SEP.1
FIA_UAU.2[Appli]	FMT_MOF.1	FPT_RVM.1	FPT_SEP.1
FIA_UID.2[Appli]	FMT_MOF.1	FPT_RVM.1	FPT_SEP.1
FIA_AFL.1[Appli]	FMT_MOF.1	FPT_RVM.1	FPT_SEP.1
FIA_SOS.1[Appli]	None	FPT_RVM.1	FPT_SEP.1
FDP_ETC.1	None	FPT_RVM.1	FPT_SEP.1
FDP_ACC.1[Disk_eject]	FMT_MOF.1	FPT_RVM.1	FPT_SEP.1
FDP_ACF.1[Disk_eject]	FMT_MOF.1	FPT_RVM.1	FPT_SEP.1
FMT_MSA.3	None	FPT_RVM.1	FPT_SEP.1
FDP_ACC.1[Cover_open]	FMT_MOF.1	FPT_RVM.1	FPT_SEP.1
FDP_ACF.1[Cover_open]	FMT_MOF.1	FPT_RVM.1	FPT_SEP.1
FMT_MSA.1	FMT_MOF.1	FPT_RVM.1	FPT_SEP.1
FMT_SMR.1	FMT_MOF.1	FPT_RVM.1	FPT_SEP.1
FMT_SMF.1	FMT_MOF.1	FPT_RVM.1	FPT_SEP.1
FIA_USB.1	FMT_MOF.1	FPT_RVM.1	FPT_SEP.1
FIA_ATD.1	FMT_MOF.1	FPT_RVM.1	FPT_SEP.1
FMT_MTD.1	FMT_MOF.1	FPT_RVM.1	FPT_SEP.1
FMT_MOF.1	---	FPT_RVM.1	FPT_SEP.1
FPT_RVM.1	FMT_MOF.1	---	FPT_SEP.1
FPT_SEP.1	FMT_MOF.1	FPT_RVM.1	---

Deactivation prevention

As shown on “Table 23: Interrelationships among security functional requirements”, FMT_MOF.1 allows only the administrator to deactivate the following functional requirements; FIA_UAU.2[Panel], FIA_UID.2[Panel], FIA_AFL.1[Panel], FIA_UAU.2[Appli], FIA_UID.2[Appli], FIA_AFL.1[Appli], FDP_ACC.1[Disk_eject], FDP_ACF.1[Disk_eject], FDP_ACC.1[Cover_open], FDP_ACF.1[Cover_open], FMT_MSA.1, FMT_SMR.1, FMT_SMF.1, FIA_USB.1, FIA_ATD.1, FMT_MTD.1, FPT_RVM.1, FPT_SEP.1. Thus, they are prevented from being deactivated by any one except the administrator.

Bypass prevention

The all functional requirements listed in “Table 23: Interrelationships among security functional requirements” do not work properly if they are bypassed, therefore, they should prevent themselves from being bypassed. The security functions called by FRT_RVM.1 ensure that the prevention is achieved successfully. In this ST, there is no functional requirement that does not need the bypass prevention.

Tampering prevention

The all functional requirements listed in “Table 23: Interrelationships among security functional requirements” do not work properly if they are interfered or tampered, therefore, they should prevent themselves from being interfered or tampered. To ensure the prevention, FPT_SEP.1 keeps their security domains unchanged and separates each domain from others completely. In this ST, there is no functional requirement that does not need the tampering prevention.

In this way, the interrelationships among all security functional requirements are adequate.

8.2.5 Adequacy of Minimum Strength of Function

This TOE is installed in an average office room and connected to the internal network. The network is connected to external network being secured by a router and firewall. Therefore it is not likely that the TOE is accessed directly by general public from outside. The internal persons who may try malicious attempts against TOE as described in “Table 2: Parties involved with TOE”, are assumed that they are not information processing specialists. Therefore, providing security functions against low-level attacks are enough and thus it can be said that the SOF-basic is adequate as the TOE minimum function strength.

8.2.6 Adequacy of Evaluation Assurance Level

Even though this TOE has less chance to be attacked by general public, the TOE handles in many cases confidential information such as medical records at hospitals, client information. Therefore, EAL3 security assurance requirement, which includes development stage analysis, components management, development security, and test, is considered as the adequate assurance level.

8.2.7 Rationale for Security Assurance Requirements

Because this TOE is used at an average office, there is a few chance that the TOE is attacked. This allows the TOE to consider only about low-level attacks. To counter the possible low-level attacks, the range of security evaluation is determined as follows; within the range that is covered by the TOE development security objectives analysis (systematic analysis and test for the development with a safe development environment). Therefore, evaluation assurance level 3 is adequate.

8.2.8 Rationale for Security Functional Requirements Consistency

The following explains the reasons for the consistency; how the security functional requirements do not conflict with each other.

- There are two identify authentication requirements, however, they are completely different and separate from each other as shown in “Table 15: Security Functions and Security Requirements”; one is used for the accesses from the control panel, and the other one is used for those from Total Disc Maker, Total Disc Monitor, or PP-100N Web application.

- There are three access control requirements; 1) for taking out discs, 2) for deactivating the electronic lock, and 3) for operating the setting control data. However, each of them controls different object, therefore, they are not conflicted with each other.

8.3 TOE Summary Specification Rationale

This section describes the rationale for the TOE summary specification; reasons for necessity and adequacy of the TOE security functions, and adequacy of the assurance measures and function strength.

8.3.1 Needs of TOE Security Functions

The correspondency between the TOE security functions and TOE security function requirements are shown in “Table 15: Security Functions and Security Requirements”. As indicated by the table, all TOE security functions correspond to at least one TOE security functional requirement. Therefore, need for the TOE security functions are satisfied.

8.3.2 Sufficiency of TOE Security Functions

FAU_ARP.1 Security alarm

The SF. Warning function warns the administrator about the possibility of security problem using the following methods.

- Sounds a buzzer
- Turns on the ERROR LED
- Displays a solution on the LCD

Thus, FAU_APP.1 is satisfied.

FAU_SAA.1 Security problems possibility analysis

The SF. Warning function analyzes the possibility of security problem when any of the following events is found.

- Published discs are detected inside the PP-100N during a power-off process.
- The disc cover is left unlocked.
- The autoloader dropped discs.
- During the PP-100N is powered, discs are detected in Stacker 2 after the stacker is removed and reattached.

Thus, FAU_SAA.1 is satisfied.

FAU_GET.1 Event log acquisition

The SF. Warning function acquires the event logs for the following cases.

- Published discs are detected inside the PP-100N during a power-off process.
- The disc cover is left unlocked.

- The autoloader dropped discs.
- During the PP-100N is powered, discs are detected in Stacker 2 after the stacker is removed and reattached.

Thus, FAU_GET.1 is satisfied.

FIA_UAU.2[Panel] User authentication before any action

When the TOE is accessed from the control panel, the SF. Identify Authentication [Panel] function requires the user to enter the user password [Panel] and authenticates the user. Thus, FIA_UAU.2[Panel] is satisfied.

FIA_UID.2[Panel] User identification before any action

When the TOE is accessed from the control panel, the SF. Identify Authentication [Panel] function requires the user to enter the user identifier [Panel]. Thus, FIA_UID.2[Panel] is satisfied.

FIA_UAU.7[Panel] Protected authentication feedback

The SF. Identify Authentication [Panel] function displays the same number of asterisks (*) as the entered password characters on the LCD. Thus, FIA_UAU.7[Panel] is satisfied.

FIA_AFL.1[Panel] Authentication failure handling

If the SF. Identify Authentication [Panel] function failed the user authentication three times in a row during a given time, the function rejects any access attempts of the administrator for six hours, or of the other users for one hour. Thus, FIA_AFL.1[Panel] is satisfied.

FIA_SOS.1[Panel] Verification of secrets

The SF Setting Data Control function verifies if the entered password satisfies the following.

- Password [Panel]: five or more numeric characters

Thus, FIA_SOS.1[Panel] is satisfied.

FIA_UAU.2[Appli] User authentication before any action

When a TOE access request comes from PP-100N Web application, the SF. Identify Authentication [Web_app] function prompts the user to enter his/her password and requests to complete the authentication. The SF. Identify Authentication [Cli_app] function performs the same thing when a TOE access request comes from Total Disc Maker or Total Disc Monitor. Thus, FIA_UID.2[Appli] is satisfied.

FIA_UID.2[Appli] User identification before any action

When a TOE access request comes from PP-100N Web application, the SF. Identify Authentication [Web_app] function prompts the user to enter his/her user identifier [Appli]. The SF. Identify Authentication [Cli_app] function performs the same thing when a TOE access request comes from Total Disc Maker or Total Disc Monitor. Thus, FIA_UID.2[Appli] is satisfied.

FIA_AFL.1[Appli] Authentication failure handling

If the SF. Identify Authentication [Web_app] and SF. Identify Authentication [Cli_app] functions failed the user authentication three times in a row during a given time, they reject any access attempts of the administrator for six hours, or of the other users for one hour. Thus, FIA_AFL.1[Appli] is satisfied.

FIA_SOS.1[Appli] Verification of secrets

The SF Setting Data Control function verifies if the entered password satisfies the following.

- Password [Appli]: five or more alphanumeric characters or special characters (“.”, “–“, “_”)

Thus, FIA_SOS.1[Appli] is satisfied.

FDP_ETC.1 Export of user data that has no security attribute

According to the access control SFP, the SF. Controlled Distribution function ejects the published discs to Stacker 4 which exists outside the control of TSF. Thus, FDP_ETC.1 is satisfied.

FDP_ACC.1[Disk_eject] Subset access control, FDP_ACF.1[Disk_eject] Security attribute based access control

According to the security attributes (user identifier[Appli], Job ID) controlled by the Controlled Distribution SFP, the SF. Controlled Distribution function allows the user to check the disc position information for the published discs. Thus, FDP_ACC.1[Disk_eject] and FDP_ACF.1[Disk_eject] are satisfied.

FMT_MSA.3 Static attribute initialization

The SF. Controlled Distribution function associates a unique user identifier [Appli] and job ID with job information, which is an object of the Controlled Distribution SFP, and also associates the unique job ID with the disc position information. The default of these security attributes (user identifier [Appli] and job ID) cannot be changed. Thus, FMT_MSA.3 is satisfied.

FDP_ACC.1[Cover_open] Subset access control, FDP_ACF.1[Cover_open] Security attribute based access control

According to the security attribute (administrator authority) controlled by Cover Open Restriction SFP, the SF. Electronic Lock Open function allows the user to deactivate the electronic lock. Thus, FDP_ACC.1[Cover_open] and FDP_ACF.1[Cover_open] are satisfied.

FMT_MSA.1 Management of security attributes

The SF. Setting Data Control function allows only the administrator to manage the security attribute. Thus, FMT_MSA.1 is satisfied.

FMT_SMR.1 Security roles

The SF. Setting Data Control function defines each user role, associates the defined role to each user, and keeps the roles unchanged. Thus, FMT_SMR.1 is satisfied.

FMT_SMF.1 Specification of Management functions

The SF. Setting Data Control function allows authorized administrators to manage the management requirements of each functional requirement. Thus, FMT_SMF.1 is satisfied.

FIA_USB.1 User-subject binding

The SF. Setting Data Control function associates users with their defined roles. Thus, FIA_USB.1 is satisfied.

FIA_ATD.1 User attribute definition

The SF. Setting Data Control function defines the administrator authority and the user identifier [Appli], and keeps them unchanged. Thus, FIA_ATD.1 is satisfied.

FMT_MTD.1 Management of TSF data

The SF. Controlled Distribution function controls so that only the users who created the discs can change or delete the disc position information. The SF. Setting Data Control function manages each TSF data accessible from the administrator, the approver, the person in charge of publishing discs, and the other users. Thus, FMT_MTD.1 is satisfied.

FMT_MOF.1 Management of security functions behavior

The SF. Setting Data Control function allows only the administrator to set the security functions. Thus, FMT_MOF.1 is satisfied.

FPT_RVM.1 Non-bypassability of the TSP

When the user ejects the published discs created by the user, the SF. Controlled Distribution function ensures that the access control is called by the TOE and completed successfully. When the administrator performs a series of operations to open the disc cover, the SF. Electronic Lock Open function ensures that the access control is called by the TOE and completed successfully. The SF. Identify Authentication [Panel], SF. Identify Authentication [Web_app], and SF. Identify Authentication [Cli_app] functions ensure that the user authentication is called by the TOE and completed successfully before any TSC function is operated. Whenever an access to the setting control information, job information, or disc position information is requested, the SF. Setting Data Control function ensures that the access control is called by the TOE and completed successfully. Thus, FPT_RVM.1 is satisfied.

FPT_SEP.1 TSF domain separation

The SF. Controlled Distribution, the SF. Electronic Lock Open, the SF. Identify Authentication [Panel], the SF. Identify Authentication [Web_app], the SF. Identify Authentication [Cli_app], the SF. Warning, and the SF. Setting Data Control functions separate the TSF from subject domains and keep them unchanged in order to protect each functional requirement from being illegally accessed or tampered. Thus, FPT_SEP.1 is satisfied.

8.3.3 Rationale of the Function Strength

In this TOE, the security functions that are realized by probabilistic or permutational mechanisms are the SF. Identify Authentication [Panel], the SF. Identify Authentication [Web_app], the SF. Identify Authentication [Cli_app], and the SF. Setting Data Control functions. These security functions indicate SOF-basic. The minimum strength level of this TOE is also SOF-basic, therefore, there is no contradiction.

8.3.4 Adequacy of Assurance Measures

The following “Lists of Document issued as TOE Security Assurance Measures” shows the correspondences between the assurance measures and security requirements.

Table 24: Lists of Document issued as TOE Security Assurance Measures

Classification	Component	Document name and TOE	Contents
ACM (Assurance Configuration Management)	ACM_CAP.3	- KP-01 PP-100N Configuration Management Plan (overall product) - KP-02 PP-100N Configuration Management Plan (mechanism) - KP-03 PP-100N Configuration Management Plan (autoloader board) - KP-04 PP-100N Configuration Management Plan (server system software) - KP-05 PP-100N Configuration Management Plan (autoloader firmware) - KL-01 PP-100N Configuration List (overall product) - KL-02 PP-100N Configuration List (mechanism) - KL-03 PP-100N Configuration List (autoloader board) - KL-04 PP-100N Configuration List (server system software) - KL-05 PP-100N Configuration List (autoloader firmware)	Necessary rules and procedures are described to ensure the TOE components integrity.
	ACM_SCP.1	- KL-01 PP-100N Configuration List (overall product) - KL-02 PP-100N Configuration List (mechanism) - KL-03 PP-100N Configuration List (autoloader board) - KL-04 PP-100N Configuration List (server system software) - KL-05 PP-100N Configuration List (autoloader firmware)	

ADO (Assurance Delivery and Operation)	ADO_DEL.1	- PP-100N Delivery Procedure Manual - PP-100N Web Delivery Procedure Manual	Delivery procedures from developers to users are described.
	ADO_IGS.1	- PP-100N Security Administrator's Guide - Install Manual for PP-100N - Sheet, Security, PP100N	All necessary procedures for safety installation and operation of TOE are described.
ADV (Assurance Development)	ADV_FSP.1	- Seiko Epson PP-100N Security Control Unit Functional Specifications - Seko Epson PP-100N Security Control Unit TOE Functions Diagram	TSF behaviors, TSF interfaces and external interfaces for functions other than TSF are described.
	ADV_HLD.2	- Seiko Epson PP-100N Security Control Unit High-Level Design Specifications - Seiko Epson PP-100N Security Control Unit TOE Subsystem Diagram	From the subsystem standpoint, the TSF configuration and interfaces for the subsystems are described.
	ADV_RCR.1	- Seiko Epson PP-100N Security Control Unit Representation Correspondence Analysis Report	Analysis of the relationship between the ST summary specifications; security functions and functional specifications, and subsystems on the High-Level Design Specifications.
AGD (Assurance Guidance Document)	AGD_ADM.1	- PP-100N Security Administrator's Guide - Sheet, Security, PP100N	All necessary procedures for safety installation and operation of TOE are described.
	AGD_USR.1	- PP-100N Security User's Guide	
ALC (Assurance Life Cycle support)	ALC_DVS.1	- PP-100N Security Control Unit Security Standard of Development	Measures to ensure the confidentiality and integrity of the TOE designing and implementation under the development environment are described.

ATE (Assurance Test)	ATE_COV.2	- PP-100N Security Control Unit Functional Test Report - PP-100N Security Control Unit High-Level Design Test Report	The followings are described; functional test items and the procedure to verify that the TSF is executed as specified, the expected test result, and the actual test result.
	ATE_DPT.1		
	ATE_FUN.1		
	ATE_IND.2		
AVA (Assurance Vulnerability Assessment)	AVA_MSU.1	- PP-100N Security Control Unit Analysis Report on improper use	The result of analysis on improper use are described. The analysis were carried out for minimizing the risk that the TOE administrator is ignorant of a TOE security problem.
	AVA_SOF.1	- PP-100N Security Control Unit Functional Strength Analysis Report	The result of analysis on the functional strength of the following functions are described; TOE security functions that are realized by probabilistic or permutational mechanisms except the encryption mechanism
	AVA_VLA.1	- PP-100N Security Control Unit Vulnerability Analysis Report	The result of analysis on vulnerability are described. The analysis was carried out for searching if any apparent security vulnerability exists and for confirming that the vulnerability is not abused in the intended TOE environment.

As shown in the above list, a set of document issued as TOE security assurance measures is provided for each TOE security assurance requirement. The document covers all the evidences required by the TOE security assurance requirements defined by this ST.

8.4 PP Claims Rationale

There is no reference PP.